THE EU DATA PROTECTION DIRECTIVE: IMPLICATIONS FOR THE U.S. PRIVACY DEBATE

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

MARCH 8, 2001

Serial No. 107–19

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

71–497PS WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

NATHAN DEAL, Georgia
Vice Chairman
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDOLPHUS TOWNS, New York
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

THE EU DATA PROTECTION DIRECTIVE: IMPLICATIONS FOR THE U.S. PRIVACY DEBATE

THURSDAY, MARCH 8, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Sterns, Deal, Shimkus, Bryant, Buyer, Radanovich, Pitts, Bono, Walden, Bass, Tauzin (ex officio), Towns, DeGette, Doyle, Markey, and Gordon.

Staff present: Ramsen Betfarhad, majority counsel; Yong Choe, legislative clerk; and Bruce M. Gwinn, minority counsel.

Mr. STEARNS. Subcommittee on Commerce, Consumer Protection, and Trade will convene.

I like to start as much as possible right on time, so I hope we will start a precedent, so that members will understand that if we arrive early then we get things moving, and then we don't have to spend as much time here waiting.

I welcome you all to the second hearing of the Subcommittee on Commerce, Trade, and Consumer Protection of the Energy and Commerce Committee. I especially want to acknowledge our distinguished guests from Europe, Professor Stefano Rodotà, the president of the Italian Data Protection Commission and chairman of an EU Data Protection Working Group; and Mr. David Smith, Assistant UK Information Commissioner.

I thank you for making the long journey and am pleased to have distinguished European officials such as yourself addressing our subcommittee. So thank you.

My colleagues, the purpose of today's hearing is twofold. First, we seek to learn more about the European approach to information privacy. Second, we wish to consider the impact of the European Data Protection Directive on international commerce in general and e-commerce specifically.

In highlighting the EU Data Protection Directive for consideration today, I hope we can get answers to the following questions. What is the directive? How is it implemented? How is it enforced? What, if anything, can we in the United States involved in the information privacy debate learn from the directive which encap-

sulates the European approach to information privacy? What implications does the directive harbor with relation to international commerce; specifically, transatlantic commerce? And what is the import of safe harbors and model contracts?

My colleagues, the answers to these questions have significant implications for companies who want to do business in and with Europe. This hearing not only represents the subcommittee's second in a series of privacy hearings, but also represents the first hearing under the subcommittee's trade jurisdiction.

In a coming week or 2, I expect to unveil the topic and time table of as many as five subcommittee hearings addressing the information privacy issue. Moreover, the subcommittee, as part of its trade jurisdiction, will begin to examine legal and regulatory measures that may impede the growth of e-commerce globally.

I rely on the words of one of our witnesses in highlighting the significance of our inquiry today when he said, "The EU privacy directive is probably the most important law by which the EU is writing the rules of cyberspace."

Mr. Winer is not alone in his concern. Many large transnational and even U.S. businesses with modest international operations have expressed the same concerns to me and other members in private.

Raising issues of significant import to our increasing knowledge and information-based economy in my office is one thing. Raising those issues in a congressional hearing is a totally different matter. I encourage all companies and interested parties to engage and speak their views openly on this issue while we are still defining the parameters.

I am concerned about the potentially regressive impact of the directive and its implementing statute now in effect in 11 out of the 15 member states on international commerce, and more specifically on commerce between the European community and the United States. I am not convinced, nor is corporate U.S. America, that the safe harbor provisions negotiated by Ambassador Aaron in the previous administration will help mitigate the concern over regressive effects.

The Ambassador has accurately noted, "While we and the Europeans share many basic values, the European Union directive comes from a different legal tradition and historical experience." The safe harbor principles are reflective of those European traditions and experiences, and as such at times don't harmonize well with our American legal tradition and historical experiences.

I encourage President Bush and the administration to begin the examination of this important issue on an expedited basis. By way of holding this hearing, we, as members of both the subcommittee and the full Energy and Commerce Committee, want to stress our keen interest in the trade ramifications of the directive. We will follow this issue carefully, and if need be we will make our wishes known in more definitized ways.

And with that, I am pleased to recognize the ranking member, Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman, for holding this hearing. I think this is a very, very important hearing, and I

want to salute you for that. And I would also like to ask permission to put my entire statement in the record.

Mr. STEARNS. Without objection, so ordered.

Mr. TOWNS. We have all heard the terrible abuses that have occurred when personal information is misused. A person's job can be lost, their creditworthiness can be destroyed, and their personal peace of mind can also be destroyed.

But privacy is not only a problem for consumers; it is a major issue for business as well. While privacy policies can limit business marketing opportunities, the effect of privacy policies on consumer confidence is a far more important fact in the future success of e-commerce.

Today we will hear how the European Union has chosen to balance commercial and consumer privacy interests. And as in so many cases, we will learn how regulations in one country can threaten the ability of U.S. firms to engage in foreign commerce. Compliance with the EU Privacy Directive is not optional.

In order to transfer personal data on any type out of the EU, a U.S. firm will soon be forced to comply. A firm that fails to comply can be blocked from transferring data out of the European Union.

In conclusion, Mr. Chairman, let me say I am not interested in defending either the EU Privacy Directive or the safe harbor agreement. That is not my interest. However, I do believe that privacy protections need to be uniform, and they need to be transparent. Consumers should not have to hire law firms and investigators and negotiators to identify privacy protections that companies have agreed to provide in private contracts.

Furthermore, no consumer, no matter where they live, is due any less than the highest privacy protection a company provides to any other consumer. When a company agrees to a particular privacy policy, it should provide everyone it serves with those same benefits.

Finally, any privacy policy is meaningless unless it is enforceable. Therefore, government has an important part to play in making privacy enforceable.

Mr. Chairman, I look forward to working with you on these matters. Consumers all over the world are demanding greater control over their personal data. This Congress has an important role to play in making sure consumers get the privacy protection they deserve, and I am certain that you will provide leadership in that regard.

I yield back.

[The prepared statement of Hon. Edolphus Towns follows:]

PREPARED STATEMENT OF HON. EDOLPHUS TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. Chairman, I want to thank you for holding this important hearing. Privacy is clearly one of the highest priority consumer protection issues we face. We have all heard the terrible abuses that have occurred when personal information is misused. A person's job can be lost. Their creditworthiness can be destroyed, as can their peace of mind.

But privacy is not only a problem for consumers; it is a major issue for business. While privacy policies can limit business marketing opportunities, the effect of privacy policies on consumer confidence is a far more important factor in the future success of e-commerce.

A survey conducted by AT Kearney management consultants and reported in November of last year in the publication "BizReport" confirms this point. Let me quote, "E-retailers worldwide lose $6.1 billion in sales, due to an 80 percent failure rate among online purchase attempts . . ." and that "Invasive information requests are blamed for 52 percent of sales that fall apart, followed by reluctance to enter credit card data (46 percent) . . " Clearly, business is paying a big price for the confidence consumers lack in the privacy and security of their online transactions.

Today, we will hear how the European Union (EU) has chosen to balance commercial and consumer privacy interests. And, as in so many cases, we will learn how regulations in one country can threaten the ability of U.S. firms to engage in foreign commerce. Compliance with the EU privacy directive is not optional. In order to transfer personal data of any type out of the EU, a U.S. firm will soon be forced to comply. A firm that fails to comply can be blocked from transferring data out of the EU.

Because the U.S. has no comprehensive national privacy policy, much less one that is comparable to the EU directive, the EU has decided that all American firms lack adequate privacy protections for personal data. The privacy provisions of the recently enacted financial modernization legislation do not, according to the EU and many others, provide adequate privacy protection. U.S. firms, therefore, are in a bind.

Recognizing this fact, the EU and the U.S. entered into a Safe Harbor Agreement last year. The Safe Harbor has one purpose. It allows certain U.S. firms to declare their compliance with agreed upon privacy protections that the EU does consider to be "adequate," so that U.S. data firms can continue doing business in Europe.

The way it works is that U.S. firms, and I am happy to say that one such firm—Hewlett Packard—is represented here today at this hearing, must certify to the Department of Commerce that they comply with the privacy protections in the Safe Harbor. Everything is public and is open for consumers and all to see. The Commerce Department's web site has both the privacy principles as well as the names of the 27 entities who, so far, have certified they comply with the Safe Harbor.

Certain firms cannot take advantage of the Safe Harbor's protection. Financial institutions—banks, securities firms, and insurance companies—do not have safe harbor protection at this time. In fact, some financial and other firms have actually organized in an effort to convince the EU and the U.S. to terminate the Safe Harbor altogether.

Instead, the only way for financial firms currently to comply is through the negotiation of private contracts either with their EU customers directly or with EU privacy officials in each country where they operate. It is unfortunate that we do not have a U.S. financial or other firm with us today who can tell us about the privacy contracts that have been negotiated. Although we may assume, we do not actually know the extent to which these contracts comply with the privacy directive. We also do not know the extent to which U.S. firms are offering EU consumers privacy protections they deny their U.S. consumers. Hearing from someone in the financial services industry could have helped clarify these matters.

In conclusion Mr. Chairman, let me say, I am not interested in defending either the EU privacy directive or the Safe Harbor Agreement. However, I do believe that privacy protections need to be uniform, and they need to be transparent. Consumers should not have to hire law firms and investigators to identify privacy protections that companies have agreed to provide in private contracts.

Furthermore, no consumer, no matter where they live, is due any less than the highest privacy protection a company provides to any other consumer. When a company agrees to a particular privacy policy, it should provide everyone it serves with those same benefits. Finally, any privacy policy is meaningless unless it is enforceable. Government, therefore, has an important part to play in making privacy enforceable and uniform.

Mr. Chairman, I look forward to working with you on these important matters. Consumers all over the world are demanding greater control over their personal data. This Congress has an important role to play in making sure consumers get the privacy protection they deserve.

Mr. STEARNS. I thank my colleague.

Mr. Shimkus, gentleman from Illinois?

Mr. SHIMKUS. Thank you, Mr. Chairman. We appreciate this hearing, and I think it has great implications, as everyone has said.

The UE Privacy Directive has important implications for U.S. companies who are doing or want to do business with Europe and

with our largest trading partner. But I want to put on record my concern, after hearing the decision rendered by the European Court of Justice earlier this week, that allows the European Union to lawfully suppress political criticism of institutions and of leading figures.

In this country, in the history of our country, we have basically had some distrust of national government, symbolically, in the creation of the Bill of Rights to our Constitution over 200 years ago. In so doing, the first one being the First Amendment, freedom of speech, what the implication is here is that our—probably our strongest allies and democratic countries may not have that faith and trust in the freedom of expression, of political expression.

This decision is very disturbing, one that could have major implications on the privacy issue and an impact on future business relations between the U.S. and EU companies. And I hope that we will have some addressing of this issue in this hearing.

I do appreciate the long distance you all have traveled. I just did the same trip 3 weeks ago as a member of the NATO Parliamentary Assembly. We visited the UE Commission, and I think next year we're going to have a chance to visit the UE Parliament with discussions on transatlantic issues of great importance to us. But I think this hearing is very, very important, and I look to be a full participant.

And I thank the Chairman and yield back my time.

Mr. STEARNS. I thank my colleague.

The gentleman from New Hampshire, Mr. Bass?

Mr. BASS. No statement.

Mr. STEARNS. The gentleman from Indiana, Mr. Buyer?

Mr. BUYER. No statement.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

I want to start by thanking Subcommittee Chairman Stearns for calling the first ever Congressional hearing, in either the House or Senate, specifically focused on the EU Privacy Directive. The topic of today's hearing is extremely relevant to the Committee's consideration of privacy and information exchange issues.

The development of electronic commerce has accentuated the fact that the U.S. economy is interdependent on the rest of the world. The Internet and other electronic networks expand the ability of businesses to reach new or untapped markets worldwide. These technologies fundamentally shrink the size of the globe. Policies affecting electronic commerce made by the world's largest trading block—the European Union—have an impact on the U.S. It also has an impact on how the U.S. Congress will approach the debate over privacy.

The U.S. and EU Member States approach the issue of privacy from different perspectives. Europeans are instilled with the belief that privacy is a fundamental human right. There are a number of reasons for this belief, including the vast and traumatic experiences of the Nazi regime during the 1940's. Another reason for this perspective is the simple fact that many EU countries are relatively new democracies. It was not long ago that Kings and Queens ruled throughout Europe. In the U.S., we take a different approach towards privacy as we have fundamental protections to free expression provided in the U.S. Constitution, including the First Amendment. By in large, we also rely heavily on the private sector to protect consumer privacy.

I believe that the EU Privacy Directive may act as a de-facto privacy standard on the world. It may or may not be permissible under the WTO because of the technical structure and specific carve-outs, but it certainly is an effort to impose the EU's will on the U.S. While I recognize that similar charges have been laid against certain U.S. policies, the EU Privacy Directive could be the imposition of the one of the largest free trade barriers ever seen and is a direct reversal of the efforts

we have made in various free trade agreements. It certainly provides for extraterritorial enforcement of EU principles on Americans and American companies.

I have serious reservations about the real impact of the EU Privacy Directive on commerce and trade. I am very concerned that U.S. companies, which have been the creators and the leaders of E-commerce, will be forced to deal with such a restrictive concept. I would love for someone to provide some type of compliance cost analysis for the Privacy Directive but that simply hasn't been done. I suspect the costs would be in the multi-billions, and are all costs that will be passed onto consumers.

One of the many drawbacks of imposing something like the Privacy Directive on the entire world is that one-size does not fit all. Europeans do not view lawsuits as an answer to problems. In the U.S., lawsuits are filed at the drop of a hat. A stock dropped too much or too fast, a lawsuit gets filed. A neighbor's dog barks too loud, a lawsuit gets filed. That is a reality that we have to deal with. However, such lawsuits could cripple the beneficial exchange of information that is a cornerstone of American business practices today.

Compliance and enforcement of the Privacy Directive has, at best, been spotty in European nations. In fact, a number of nations have not even bothered to required enact implementing legislation. This lax attitude is something that Americans are not used to. We do not build elaborate restrictions with a wink and a nod so they can be ignored. Given this, we need to know whether enforcement of the Privacy Directive on U.S. companies represent a double standard when compared to enforcement of European firms. We also need to know the consequences for competition if this occurs.

I must admit that I take a dim view about the way that the EU went about enacting this new privacy regime. The EU designed the rules and told the U.S. companies to abide by them or risk losing the transfer of any data from European nations. In essence, do it or suffer the consequences. There was no international negotiations. The U.S. was allowed to participate in negotiations resulting in the so-called "Safe Harbor" but it is interesting to note that very few firms have signed up for it.

The Safe Harbor raises a whole host of issues in and of itself. For instance, the legal status of the Safe Harbor is highly questionable. Further, the Safe Harbor doesn't cover financial firms. Indications are that privacy provisions of the "Gramm-Leach-Bliley" Financial Services Modernization Act are not "adequate" for purposes of the Privacy Directive. This is non-sense, as many people make a compelling case that these provisions are too strong. More importantly, what are global financial firms to do? They don't qualify for the Safe Harbor and U.S. law, which they must obey, is being overrun by the Privacy Directive.

Recently, the EU has been designing so-called "model contracts" that can be used to meet the stringent requirements of the Privacy Directive. Many experts have suggested that the model contracts will be imposed on U.S. firms as a way to "top-off" or strengthen the Safe Harbor. This seems to directly contradict the purpose of the Safe Harbor and the negotiations that took place. Was the Department of Commerce duped into supporting the Safe Harbor? Are the Europeans really trying to find ways to strengthen the Privacy Directive?

I am hopeful that this hearing will provide some insight and provide some comfort regarding the EU Privacy Directive. Unless or until that occurs, I think it only appropriate to consider all the options this Committee can take. Many have asked for our assistance in steering the new Administration towards the proper perspective on this issue. I think we should give serious consideration to doing just that.

PREPARED STATEMENT OF HON. MIKE DOYLE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA

Mr. Chairman, thank you for calling this hearing to discuss the issue of personal data privacy as it relates to international e-commerce and trade. E-commerce transcends global boundaries at light-speed, literally bringing the world to individual consumers and industries and offering an unprecedented opportunity for advancement and economic growth.

During last week's hearing, I voiced my concerns that in the past, over-zealous federal regulations sometimes created unnecessary burdens on business. I firmly believe that it is the responsibility of the federal government to find the most appropriate balance that ensures we do not unintentionally choke out our emerging high-technology e-commerce sector while at the same time providing floor requirements relating to basic privacy protections for consumers and industry alike.

And while I find the European Union approach towards personal data protection noble insofar as they recognize the importance of an individual's control over the

sharing of personal information, it goes without saying that applying such government actions here in the United States would raise some troublesome issues and almost surely conflict with the Constitution.

But, if we in America do not act to establish some general requirements to ensure the integrity of personal privacy for our citizens and global consumers, both Americans and Europeans may very well risk losing out on vast economic opportunities.

Here in the United States, the Safe Harbor provisions represent a good start, but lack they comprehensive application to all sectors of our economy. In my view, it is important that the same, uniform minimum standards are applied to all transactions involving online personal privacy, regardless of the particular economic sector they may fall.

While the European Union Privacy Directive is a source of concern to me on various levels, I do believe that it serves, as does this hearing, as a catalyst for discussion and implementation of real online personal privacy protections.

No doubt that several US firms, separate from the Safe Harbor principles, have negotiated with the European Union to ensure the security of personal data is maintained when conducting transatlantic e-commerce. Such aggressive industry self-regulation is just the type of proactive, responsible action that assuages consumer unease and concern with e-commerce privacy.

In my view, an effective blend of industry self-regulation within a comprehensive framework of federal minimum standards must become the new standard for 21st century e-commerce in the United States if our industries and consumers are to continue to capitalize on high-technology sector growth.

Mr. Chairman, I am eager to work with you and my colleagues of the Subcommittee on ways to facilitate the prosperity global e-commerce.

PREPARED STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. Chairman, thank you for holding this important hearing on the European Union Privacy Directive. I particularly want to thank Professor Rodota and Mr. Smith for traveling such a long distance to discuss this important topic. This hearing is significant for two reasons.

First, ensuring an ongoing dialogue between the European Union and the United State regarding the EU's Privacy Directive and its underlying purpose is critical for ensuring continued and uninterrupted trade between our nation and the countries which make up the European Union. The European Union is one of our most valued trade partners. However, it is clear that the United State's privacy laws in many sectors of our economy do not meet the strict standards of the European Union Privacy Directive. Only by working together can we ensure that the inadequacy of U.S. privacy laws and strength of the European Union's Privacy Directives do not lead to disruption in our strong trade relationship.

Second, we in the United States can learn a great deal from the European Union's Privacy Directive. The United States does not have a comprehensive privacy policy. Some sectors of our economy have no protections what so ever. Also, in some cases, information is susceptible to misappropriation and misuse. Also, in many cases enforcement is limited to government action because no private cause of action is provided. The European Union's Privacy Directive represents an example of a strong law covering many different types of information which provides extensive enforcement mechanisms.

However, the European Union's Privacy Directive is not without its faults. Some would argue that it covers information which is clearly public. We in Congress need to learn from the European Union's efforts what works and what doesn't. It provides one of the clearest examples of what is feasible and infeasible.

I commend the witnesses from Europe for their work in this area and those witnesses who have worked with the European Union to ensure their is no disruption in the trade relationship between the United States and the European Union.

Mr. STEARNS. With that, we will have the first panel, Professor Stefano Rodotà, Chairman, European Union Data Protection Working Group, and Mr. David Smith, Office of the UK Information Commissioner.

I want to thank, again, both of you for your coming the long distances, and I look forward to your opening statement. So you can give your opening statement right now if you would. Professor, we will start with you.

STATEMENTS OF STEFANO RODOTÀ, CHAIRMAN, EU DATA PROTECTION WORKING PARTY; AND DAVID SMITH, ASSISTANT COMMISSIONER, OFFICE OF THE UK INFORMATION COMMISSIONER

Mr. RODOTÀ. Thank you, Mr. Chairman. Thank you for inviting me to testify today at this important hearing.

I am Stefano Rodotà. I am the Chairman of the Italian Data Protection Commission. I am also a professor of law, and I have been for several years a member of the Italian Parliament and of the European Parliament. So I shared the same responsibility you have now.

So I am chairman of the Data Protection Working Group established by the European directive of data protection passed by the European Parliament, as you know, and the Council in 1995. And I must say that when compared to other pieces of European legislation, the directive presents a prominent feature. It aims at protecting fundamental rights and freedoms, although this objective is twinned with the free movement of services.

This approach has been recently stressed by a major development in the charter of fundamental rights of the European Union signed in December of last year by the European Parliament, the Council——

Mr. STEARNS. Professor, could I have you pull the speaker up just a little closer to you?

Mr. RODOTÀ. Oh, yes.

Mr. STEARNS. Yes. That will be fine.

Mr. RODOTÀ. Yes, sorry.

Mr. STEARNS. No, no. That is fine. Thanks.

Mr. RODOTÀ. It is better.

Mr. STEARNS. Yes, that is better.

Mr. RODOTÀ. Oh, thank you.

So I was saying that I would like to stress that the same approach was shared by the charter of the fundamental rights of the European Union passed in December of last year by the European Parliament, the Council, and the Commission. And two specific provisions are devoted to privacy and data protection.

So now data protection must be considered a fundamental human right, and the same chart makes reference to the necessity of an independent authority.

These independent authorities, existing in all 15 countries in Europe, meet together in the Data Protection Working Party, which is also called Article 29 Group. And this group has an advisory status and acts independently, and since its creation has adopted several recommendations and opinions.

In Italy, the directive was implemented by the Data Protection Act in 1996, and then complemented by secondary legislation and, I would like to stress, by a number of codes of conduct which represent an important factor of flexibility.

I can leave you an English version of the Act, together with the articles of the European chart.

Mr. STEARNS. By unanimous consent, we will make that part of the record.

Mr. RODOTÀ. Yes. Thank you.

At that time, in 1996, Italy was the only member state of the European Union, together with Greece, without a specific data protection law. But you know what technologies say—using appropriate technologies, late comers can make a leap frog. Something like that happened in Italy. Using the European law, and transposing immediately for all the member states the directive into its legal system, Italy jumped at the top of the European data protection.

The implementation of the law has not been easy, but the societal effects are astonishing. Our Commission has been dealing during the past 4 years with nearly 100,000 offers submitted by phone, fax, e-mail, writing, and as formal requests to the Commission acting in alternative to the judiciary.

Statistically, the main people's concern regards health insurance, telecommunications, direct marketing, labor relationship, police data, banks. People can act directly toward the data controller. For instance, 4 million customers asked banks not to send them commercial advertising. The implementation of the law raised more resistances in the public administration than in the private sector that has not at all suffered the dramatic consequences foreseen by some interested circle.

So the high level of data protection legally in the UE indicates an amassing paradox. Privacy was invented in the U.S. and has long been considered to be typical of the American society. Europe now is the region of the world where maybe personal data is most protected—are most protected. This does not mean, however, that—in my opinion, that European-U.S. systems are mutually opposed.

It is an instance of misrepresentation to simplify the picture by making Europe the domain of law and the U.S. the domain of self-regulation. Indeed, it is exactly the framework provided by European directives and national laws which is making it possible to develop self-regulatory codes and contract models on a larger scale.

And at the same time, we recognize that many highly sensitive issues are being dealt with in the U.S. by means of legislative tools. We have been impressed, for instance, by the Executive Order to prohibit the use of genetic data for Federal employees. We must take this perspective seriously. We cannot accept a full-speed world in the data protection field, more and more one of the most important and critical matters in the globalized world.

Many devices can be used—national legislation, regional rules like in European Union, international guidelines, model contracts, and, finally, international conventions. We must provide a common framework.

In my double capacity, I would like to work in this area. For making possible more fruitful cooperation, the working group is now planning a visit in the U.S. mid-June.

Coming back to the directive, it has been implemented in eleven out of the 15 EU member states. Of course, the European Commission has started an infringement procedure against the four member states that have not yet notified the implementing measures—France, Germany, Ireland, and Luxembourg.

However, if we consider both the core principles and the creation of supervisory authorities, I would say that almost all member states are now in line with the fundamentals of the directive.

Germany and France are, for different reasons, in a similar paradox. They are late in passing the implementing measures. However, their data protection legislation is sound and well established. According to some observers, this paradox shows that adapting old laws may prove harder than passing a brand-new law.

The Netherlands seem to have experienced one of the most interesting parliamentary debates. This was prompted by an amendment aimed at excluding the private sector from the jurisdiction of the Data Protection Authority. The business community argued that they would feel more comfortable with the powers of self-disciplinary bodies, but the amendment was rejected because the Dutch government found that it may have been incompatible with the directive.

So all member states share now the same values and are legally bound by the same core principles, directly connected with a strong commitment to make effective fundamental human rights in this very sensitive area.

It means that also commercial and economic interests must be evaluated in this broader context. At the same time, the directive was aware of the problem of transferring that outside the European Union. The well-known Articles 25 and 26 reflects these concerns through a reference to an adequate level of data protection. Until now only Canada, Switzerland, and Hungary have met the adequacy test in the judgment of Article 29 working party.

At the same time, Articles 25 and 26 have made possible and—made possible to buildup a completely new system based for the U.S. on the safe harbor entered in force on October 25 last year—a special opportunity given to the U.S. company. But we have also the new adequacy system, including the standard contractual clauses, and the draft by the Commission services, and that I received the positive opinion of the Article 29 working group.

In my opinion, such clauses are crucial in ensuring transborder data flow because——

Mr. STEARNS. Professor, if you don't mind, we just have——

Mr. RODOTÀ. I will stop. I am ending.

Mr. STEARNS. Sure.

Mr. RODOTÀ. Just 1 minute. Are crucial because many companies make business on a global scale and because data flows from the European Union are not linked to the U.S. Both systems will be experimented with. It will be especially interesting to evaluate the enforcement system.

It does not work, however, that here are interesting developments in the attitude of the business community. More and more privacy protection is considered a value to be offered with goods and services. Opt-in and not opt-out has been indicated as the best approach by prominent European companies during their hearing before the European Parliament last January.

So we are living in a transitional period and indeed need cooperation as wide as possible. Thank you for giving me this opportunity. May I conclude with my very best wishes for your future discussions which are crucial for the democratic values that we share.

Thank you very much.

[The prepared statement of Stefano Rodotà follows:]

PREPARED STATEMENT OF STEFANO RODOTÀ, CHAIRMAN, EU DATA PROTECTION WORKING PARTY

Mr Chairman, Honourable Members, Thank you for inviting me to testify today at this important hearing. My name is Stefano Rodotà, and I am the Chairman of the Data Protection Working Party that was established by the EU Directive on the protection of physical persons with regard to the processing of personal data. This Directive was passed by the European Parliament and the Council in 1995, that is after 5 years of fierce discussions on the proposal presented by the European Commission in 1990: passing legislation on such a complex issue is not easy—neither in the EU nor in the US, you will say . . .

Since the creation of a Data Protection Commission in Italy (1997) I also wear the hat of Privacy Commissioner, and in this capacity I would like to share with you a couple of ideas on the concrete implementation of the Directive in my country. Before doing that, may I say something about the European approach to privacy and data protection, that may explain some of the difficulties that we have experienced in bridging the gap with the approach of the US Government.

When compared to other pieces of European legislation, the Directive presents a prominent feature: it aims at protecting "fundamental rights and freedoms", although this objective is twinned with the free movement of information and services. This approach has been recently stressed by a major development: in the Charter of Fundamental Rights of the European Union, that was signed in December 2000 by the European Parliament, the Council and the Commission, two specific provisions are devoted to privacy and data protection. Let me quote them.

Article 7, Respect for private and family life.

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8, Protection of Personal Data.

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be the subject to control of an independent authority.

These independent authorities, as you know, meet together in the Data Protection Working Party, which is also called "Article 29" Group, although its powers are to be found in Article 30 of the Directive. The Working Party, that I'm honoured to chair since last year, has an advisory status and acts independently. Since its creation, it has adopted a number of Recommendations and Opinions, some of which were devoted to the different versions which led to the final shape of the "Safe Harbor". All these documents are available to the public at the following web page: http://www.europa.eu.int/comm/internal__market/en/media/dataprot/wpdocs/

The Italian experience.

In Italy, the Directive was implemented by the Data Protection Act (1996). This Act is being complemented by secondary legislation and—may I stress this aspect—by a number of Codes of conduct, which represent an important factor of flexibility. All the relevant documents are available at: http://www.garanteprivacy.it

Judging from my personal experience on the ground, I can testify that the provisions by which the Directive was implemented in Italy are being invoked on such a wide range of issues that were probably hard to imagine when the law was passed—there are over 2,000 claims pending before the Garante, covering almost all business areas and administration branches—but no company has gone out of business—nor has it suffered the dramatic consequences that were anticipated by some interested circles. In Capitol Hill, you are in a good position to know that lobbying groups sometimes tend to exaggerate the cost of new legislation. In earlier times, the same happened during the Parliamentary discussions on child labour legislation, but nobody today would argue that such legislation was not appropriate.

When the Directive was passed (1995) in Italy there was no legislation in this area, and the issue was virtually confined to the academic and literary circles. In less than 4 years, the word "Privacy" has entered into the daily vocabulary of the average Italian (without any Italian translation: the media and the man in the street just say "Privacy", and they seem to know what they mean). Sometimes I'm myself puzzled about that.

The widespread use of the word "Privacy", in Italy and in other non-English speaking countries, indicates an amazing paradox. Privacy was "invented" in the US, and has long been considered to be typical of American society. Still, Europe is nowadays the region of the world where personal data is most protected—so much so that the Charter of Fundamental Rights of the European Union has recently included data protection among fundamental human rights (see Article 8, quoted above).

This does not mean, however, that the European and the US systems are mutually opposed or absolutely irreconcilable. For instance, it is an instance of misrepresentation to simplify the picture by making Europe the domain of law and the US the domain of self-regulation. Indeed, it is exactly the legislative framework provided by EU directives and national laws which is making it possible to develop self-regulatory codes and contractual models on a large scale. At the same time, many highly sensitive issues and topics are being dealt with in the USA by means of legislative tools, as shown by the many laws passed in the US at the State level and by the Executive Order issued by Clinton on 8 February 2000 to prohibit the use of genetic data for federal employees.

The implementation of the Directive in other EU countries

The Directive has been implemented in 11 out of the 15 EU Member States. The deadline for implementation was October 1998 and of course, as in many other policy areas, the European Commission has started an infringement procedure against the four Member States that have not yet notified the implementing measures (France, Germany, Ireland and Luxembourg). It is the Commission's duty, and I strongly hope that this will help in completing the implementing process. However, if we consider both the "core principles" of data protection and the creation of Supervisory Authorities, I would say that almost all Member States are now in line with the "fundamentals" of the Directive (please, don't ask me to name the one or two countries that may still make an exception).

Germany and France are, for different reasons, in a similar paradox: they are late in passing the implementing measures; however, their data protection legislation is sound and belongs to the best established in Europe (the two were the main source of inspiration of the European Directive). According to some observers, this paradox shows that "adapting" old laws may prove harder than passing a brand new law, but the case of Germany is certainly made more complex by the Federal structure of the State, that implies several levels of discussion.

The Netherlands seem to have experienced one of the most interesting parliamentary debates. As far as I understand, this was prompted by a major initiative aimed at excluding the private sector from the "jurisdiction" of the Data Protection Authority: roughly speaking, the business community argued that they would feel more comfortable with the powers of self-disciplinary bodies, and they found sympathetic ears in the Dutch Parliament; an amendment to this purpose was tabled, but the Dutch Government found that it may have been incompatible with the Directive, and the idea was finally rejected.

The provisions of the Directive with regard to transborder data flows

A prominent feature of the EU approach, if compared to the US privacy debate, is that the Directive provides with a single framework which applies irrespective of the business sector concerned, and regardless of the nature of the data controller (public or private body), although some broad exceptions are allowed.

In the recent past, some observers have argued that, since the Directive had been drafted at the time of mainframe computers, its provisions would be outdated in the Internet era. The experience gained in the meantime points to the opposite conclusion: all the core principles established by the directive, such as the right of access, rectification, deletion and the right to damages are drafted in a way that copes with technology developments, and they work properly irrespective of the technology used to process personal data.

Incidentally, a similar debate took place with regard to the OECD Privacy Guidelines, that are based on the same core principles. At the end, as you know, the applicability of the OECD Guidelines to electronic commerce was reaffirmed by the Ministerial Conference held in Ottawa in 1998, although the Guidelines are much "older" than the Directive (OECD Guidelines: 1980, EU Directive: 1995!).

Of course, the Internet revolution carries its lot of new challenges, but these normally concern the issues of applicable law and jurisdiction, rather than the content of the substantive rules, and this is the same kind of problems that does arise in many other areas of Law.

To be concrete, may I give you one example: which law applies to the online collection of personal data from individuals of country "A" by a company established in country "B" using a server located in country "C"?

When the countries concerned are within the European Union, the answer is simple: the law of Member State "B", that is the country in which the company is established. In my opinion, this solution is well balanced:

- on the one hand, it allows data controllers to comply with one single set of rules (instead of 15 or more), and this is very business-friendly;
- on the other hand, it protects citizens from the possible circumvention of their rights: using a server located in a third country would be an easy route to circumvention, but what matters for the Directive is the country in which the economic activity of the controller is located.

This approach makes sense, as all Member States share the same values and are legally bound by the same "core" principles, enshrined in the Directive. Of course, the above applies only insofar as the data controller is established in a EU Member State: where this is not the case, the issue is far more complex. If the data controller is established in a country with "no rules" on data protection, the same approach would result in the absolute lack of guarantees for the data subject, whose personal data could be processed without any restriction.

In my opinion, there is therefore a case for an International instrument on data protection, as recently stressed in the "Venice declaration" by all the colleagues convened at the 22nd International Conference on Privacy and Data Protection.

However, in the absence of an international instrument, the Directive has established two very important safeguards:

1. By requiring that Member States apply the Directive where the data controller is established in a third country but processes personal data using equipment located in the EU territory (Article 4c);
2. By the well known "Article 25", that prompted a number of alarming articles in the US press, warning against what was called "the Great Wall of Europe": according to this provision, personal data can be transferred from the EU to third countries only if the receiving country ensures an "adequate" level of data protection. Until now, only Canada, Switzerland and Hungary have met the "adequacy test" in the judgement of the Article 29 Working Party.

I agree that Article 25 sounds like a bold provision. However, to be understood, this general rule must be read together with the many exceptions established by Article 26, which allow a significant degree of flexibility (examples: the data transfer is allowed if the individual has given his unambiguous consent, or where necessary for the performance of a contract with the data subject, or to protect his vital interests, and so on). In addition, data transfers can also take place where the controller adduces appropriate safeguards, that can be offered by way of contractual provisions.

As you probably know, standard contractual clauses have been drafted by the Commission Services and have received the positive Opinion of the Data Protection ("Article 29") Working Party. In my opinion, such clauses are crucial in ensuring transborder data flows, because many companies make business on a global scale and because data flows from the EU are not limited to the US. These clauses, when adopted, will not be mandatory but if companies choose to use them, they will be able to cut out most of the administrative loops which the contractual route otherwise requires.

The Safe Harbor

The Safe Harbor is living proof that the Directive allows significant flexibility. In finding that the SH offers adequate protection, the European Commission may have gone beyond the letter of Article 25, which refers to "domestic law" or international commitments, and has accepted a set of rules that are proposed to US companies on a voluntary basis, but I will not re-open that debate: all that I want to stress, is that on the European side there has been a lot of good will.

I understand that, until now, only twenty five US organisations have adhered to the Safe Harbor, and it is to be hoped that their number will increase, after all the commendable efforts that were deployed on both sides to secure the deal.

Mr Chairman, Honourable Members, thank you for giving me the opportunity to testify. May I conclude with my very best wishes for your future discussions, which are crucial for the democratic values that we share.

Mr. STEARNS. Thank you, Professor Rodotà.

We are going to recess now. We have possibly two votes on the House floor.

So, Mr. Smith, we will reconvene after we come back, and we ask for your patience.

And I think with the two votes it will be difficult to set a time, because I think one of them is an adjournment vote. So we will reconvene probably perhaps in about 20 minutes, 25 minutes.

[Brief recess.]

Mr. STEARNS. The Subcommittee on Commerce, Trade, and Consumer Protection will reconvene.

And, Mr. Smith, thank you for your patience, and we look forward to your opening statement.

I say to my colleagues, we are giving each of these gentlemen 10 minutes, instead of the customary 5 minutes, because of the distance they have traveled and also as a courtesy so that we can really have an impact from all of their feelings on this issue.

So, Mr. Smith, you have the floor for an opening statement.

STATEMENT OF DAVID SMITH

Mr. SMITH. Thank you very much, Chairman, and thank you for allowing me some extra time.

I am David Smith, Assistant Information Commissioner from the United Kingdom. I work for Elizabeth Franz, the UK's Information Commissioner, recently renamed Information Commissioner to reflect duties she has under the UK's new Freedom of Information Act. She was formerly Data Protection Commissioner. She continues as the UK's independent supervisory authority, and it is in that role that I am here and I will talk.

So I can't act as a representative either of the European Commission or even of the UK government. I am a representative of the UK's independent supervisory authority.

I won't go through my testimony in great detail. I am happy to answer questions in relation to it. I will just highlight one or two points.

It starts with the origins of data protection law, particularly in the UK. And as Professor Rodotà said, we do see data protection law as an aspect of human rights, individuals' rights to have some knowledge of the information that is kept and used about them, a right to some control over who has access to that information, and how they use it, and some safeguards and rules that we know businesses that keep that information will abide by.

That is exemplified in Europe in the Council of Europe Convention on Data Protection, which is at the root of all European data protection law, including the UK's law. But it bears some similarities to the OECD privacy guidelines with which you may be familiar.

But when data protection started, certainly in the UK, it was not only about human rights that was behind government thinking. It was also about building people's trust in business, going back some time in the use of computers at that time, but say, "Here is the law to protect you. You can trust businesses that computerize information." And that does have some relevance in the world of e-commerce that we are now in.

The EU Data Protection Directive is designed to harmonize European laws and to remove barriers to the flow of information within Europe. It essentially takes the Council of Europe Convention fur-

ther, makes it a mandatory requirement, and modifies it in relation to EU member states.

In addition to the general Data Protection Directive to which the attention is focused on, there is a Data Protection Directive specifically focusing on the telecommunications section, which adds to the general directive. And there is even some suggestion now, although nothing firmly proposed, that there will be one relating to the employment sector.

The UK Act implements the European directive. The Act sets out the scope of the law. It applies not only to automated computerized records. It also applies to structured manual records. It works on the basis of criteria for processing.

In order to keep—use information about individuals, a business has to meet certain criteria, which in general are not especially difficult to meet but are more onerous where the information falls into the category of sensitive data, into particular categories there.

The law gives individuals rights such as the right of access to their information and the right to compensation if the information is misused. And it sets out standards that data controllers, businesses, must follow called the Data Protection Principles, which cover the requirement to fairly process information to keep the information secure, and so forth.

One of those principles relates to international transfers, and the testimony I have provided talks about the meaning of adequacy in terms of only transferring data to countries outside Europe that provide adequate protection.

What is actually meant by "adequacy"? It doesn't necessarily require data protection law. It does depend on the nature of the data that are transferred, codes of practice, enforceable codes, and the like, that exist in the country involved. The testimony refers to community findings. Professor Rodotà referred to particular countries where there has been a finding of adequacy, and the safe harbor arrangements fall into that category.

As UK Information Commissioner, we are obliged under a community finding to accept the safe harbor arrangements as providing adequacy to companies that have signed up to it. There are exceptions to the requirement for adequacy where individuals have given their consent to the transfer of the data where the data are necessary for legal proceedings and in a number of other areas.

And I also talk in the testimony about the role of standard contracts and the work that is going on to develop those contracts to govern the transfer. So a variety of arrangements under which adequacy requirements can be satisfied.

In terms of enforcement, the UK law does not contain much in the way of criminal offenses and criminal penalties for breach. The one we place most emphasis on is that of obtaining information by deception. Essentially, people like private investigators who will contact a bank, an insurance company, a doctor, and pretend to be someone with authority to acquire information, and so, therefore, do so by deception. And we do prosecute those, and we regard that as a particularly important aspect of our law.

But generally, we enforce the law through enforcement notices which set out requirements that businesses have to undertake to comply with the law to delete data to change their practices, or

whatever. And a failure to comply with the notice is then a criminal matter for which we can prosecute. And individuals, under the law, have their own right to take action through the courts to enforce their rights.

As Information Commissioner, we see our role, and, indeed, the law sets out our role, as not being solely or even necessarily primarily about enforcement. We are very keen to develop awareness amongst citizens and amongst businesses of how the law operates and their rights and responsibilities under it.

We promote good practice which goes wider than simply complying with the law, and it covers conduct which is consistent with those requirements. And as Professor Rodotà said, we also put emphasis on the development of codes of practice, codes that develop how the law applies in the area of particular industry, particular activities, fields such as the use of data in employment.

We deal with requests for assessment from individuals, individuals who ask us to assess whether the law has been complied with, and we make those assessments. But we have a wider strategy, and I will just, in conclusion, spend a moment or two on developing our strategy. Because, as I said, we are keen to work on the basis of education and encouragement, both of individuals and of businesses.

We take a very strong view that data protection and privacy requirements should be built in at the early stage of thinking, whether that is the development of new business processes, new IT systems, or the development of public policy.

They should start with data protection in mind, and one example of work we are doing in that area is the development of guidelines for those involved in the development of IT systems on how to incorporate privacy-friendly features into those systems, part of our work of encouragement and producing guidance.

We also encourage self-regulation, not necessarily instead of statutory regulation but together with it. We see self-regulation, provided this is effective and gives effective remedies to individuals, and there are arrangements to check that businesses comply, audit arrangements, and the like, as being the best way of providing remedies for individuals and enforcing data protection day to day.

And we are supporting and actively working with the development of alternative dispute resolutions as a better method than individuals either taking their cases through the court or our office necessarily seeking to resolve them for them.

We also promote good business practice. We are encouraged by some developments, particularly in the e-commerce field, where businesses are increasingly positioning themselves for privacy, not necessarily because they see that as a way of meeting regulatory requirements, but because it is what they see as necessary to attract and retain customers, permission marketing, giving the customer choice, and the like.

And we encourage that, because the more that data protection flows out of good businesses practice than is seen as a simple additional regulatory burden, the more satisfactory and the more effective it will be.

And, last, we do seek to influence law makers as well in the UK and elsewhere to develop better protection for the privacy rights of

individuals, but to do so without imposing disproportionate burdens on businesses.

So I hope, Chairman, that is an introduction to our work and has been useful to you. Thank you for giving me the time. I am happy to answer any questions or provide further information if that would be helpful.

[The prepared statement of David Smith follows:]

PREPARED STATEMENT OF DAVID SMITH, ASSISTANT COMMISSIONER, OFFICE OF THE UNITED KINGDOM INFORMATION COMMISSIONER

SUMMARY

This testimony is intended to be informative. It is submitted on behalf of the UK Information Commissioner who is the independent supervisory authority appointed under the Data Protection Act 1998. The views expressed are those of the Commissioner and do not necessarily represent the position of either the European Commission or the UK Government.

The testimony covers:

- The Origins of Data Protection in Europe; The 1981 Council of Europe Convention, the objectives of Data Protection law and the thinking behind the UK's Data Protection Act 1984.
- The EU Data Protection Directives: The reasons for the general Directive, the timescale for its implementation and the related Telecommunications Data Protection Directive.
- The UK Data Protection Act 1998: The scope and application of the law, criteria for processing, sensitive data rules, other general provisions, individual rights and the standards to be followed by data controllers (the Data Protection Principles)
- Transfers of Personal Data to Third Countries: What is meant by an "adequate level of protection", Community findings and exceptions to the requirement for adequacy including the role of standard contracts.
- Enforcement: Criminal offences under the Data Protection Act, obtaining personal information by deception, enforcement of the Principles, information notices and the rights of individuals to take proceedings through the courts.
- The Information Commissioner: The Commissioner's functions under the Data Protection Act, the role and development of codes of practice, her duty to make assessments as to whether it is likely or unlikely that the Act's requirements have been met, her strategy in promoting compliance with the Act and more widely promoting respect for privacy and personal information both nationally and internationally, some activities she is involved in and some comments she has made in relation to possible revision of the legal framework.

ORIGINS OF DATA PROTECTION

European Data Protection law has its roots in thinking in the 1970s which led to the 1980 OECD Privacy Guidelines [1] and to the 1981 Council of Europe Data Protection Convention (Convention 108) [2]. It is Convention 108 that formed the basis for the UK and many other European Data Protection laws prior to the Directive and which is now reflected in the provisions of the Directive itself.

Article 1 of Convention 108 sets out the objective.

> "The purpose of this convention is to secure . . . for every individual . . . respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him".

At its simplest, Data Protection law delivers this objective through three strands:

knowledge: The right of the individual to be informed what personal information is kept, by whom and how it is used and the right of access to the information.

control: some control by the individual over what information is kept and how it is used.

safeguards: safeguards to ensure appropriate confidentiality, availability, integrity and security of personal information.

---

[1] Organisation for Economic Co-operation and Development, Guidelines Governing the Protection of Privacy and Transsborder Flows of Personal Data, Paris 1980.

[2] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series 108, Strasbourg 1981.

The human rights approach to Data Protection is clear. It is founded in the right to respect for one's private life. However this was not the only thinking behind either Convention 108 and the UK's Data Protection Act 1984 or the OECD Privacy Guidelines. There were two other strands, both of which are particularly relevant in the context of the development of electronic commerce and global markets. First there was the fear of technology, whether real or imagined. Evidence suggested that individuals were reluctant to trust their information to computers and there was anxiety that this lack of trust would stifle the development of technology in business. Legal protection was seen as a way of reassuring individuals.

Second was the question of transborder data flows. Fears that the lack of an international instrument would lead to restrictions on transfer by those countries with domestic law were an important factor. In the UK, the Government's reasons for promoting Data Protection legislation were given by the then Home Secretary in the House of Commons on 30th January 1984.

> "first . . . reassure people that . . . there are special safeguards for individual privacy . . .
>
> secondly . . . membership of the European Data Protection club . . . a very important commercial interest . . . British firms not placed at a disadvantage . . ."

Although Data Protection law can be seen as a means to facilitate international trade rather than as a trade barrier it has never sought to achieve this by allowing an unrestricted flow of personal data from those countries that adopt protective measures to those that do not. The UK's Data Protection Act 1984 included provision for transfer prohibition notices. Although used rarely this enabled the then Data Protection Registrar to stop the transfer of personal data to a country that was not bound by Convention 108, if the transfer was likely to lead to a contravention of the Act.

THE EU DATA PROTECTION DIRECTIVES

Not all member states of the European Union chose to be party to Convention 108. Those that did used the freedom it allowed to adopt domestic laws that varied significantly. As part of the development of an internal market within the European Union and to facilitate what was seen as a necessary and substantial increase in cross-border flows of personal data, the EU General Data Protection Directive [3] was adopted on 24 October 1995. Member states have no choice but to implement it in their domestic law. There is still scope for variation in its interpretation and application but this is much less that is the case with Convention 108.

The EU Directive takes familiar themes forward. It clearly states as its two objects:

- "... member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"
- "... member states shall neither restrict nor prohibit the free flow of personal data between member states ..."

The Directive took several years to agree. It is necessarily a compromise between the cultures, existing laws and aspirations of different member states. To comply with the Directive, member states should have had domestic law in place within three years of its adoption ie, by 24th October 1998. The UK law came into force on 1st March 2000. The Directive allows a transitional period for "processing already under way" at 24th October 1998. For most processing this transitional period will run out on 24th October 2001.

In addition to the general Directive referred to above there is a related Directive addressing Data Protection in the Telecommunications Sector [4] The intention of this directive is to particularise and complement the provisions of the general Directive as they apply in the this sector.

THE UK DATA PROTECTION ACT 1998

The general Data Protection Directive is given effect in the UK by the Data Protection Act 1998. There are separate provisions implementing the Telecommunications Directive.

---

[3] Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281, Vol. 38, 23rd November 1995, ISSN 0378-6978.

[4] Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997. Concerning the Processing of personal data and the protection of privacy in the telecommunications sector.

General Provisions

Scope: The Act applies to the processing of personal data. "Personal data" is information that relates to a living, identifiable individual. It includes information held not only in automated systems but also in structured manual records referred to in UK law as a "relevant filing system". "Processing" is defined widely and includes any operations performed on personal data from collection through to deletion.

Application: The Act regulates the activities of data controllers. That is persons who determine the purposes for which and manner in which personal data are processed. It applies to data controllers who are:

- established in the UK provided the data are processed in the context of the UK establishment even if the processing actually takes place elsewhere.
- not established on the territory of the UK or another member state but make use of equipment in the UK for processing.

Criteria for Processing: Before personal data can be processed, one of the following criteria must be satisfied:

- the data subject has consented;
- the processing is necessary for performance of a contract involving the data subject or for pre-contractual steps;
- the processing is necessary for compliance with a legal obligations;
- the processing is necessary to protect the vital interests of the data subjects;
- the processing is necessarily carried out in the public interest;
- the processing is necessary for legitimate interests pursued by the controller except where these are overridden by the need to protect the rights and freedoms of the data subject.

The Information Commissioner takes the view that regardless of whether any of the other criteria are also satisfied, legitimate business activities should generally be able to rely on the last of the above.

Sensitive Data: Where sensitive data are processed, one of an additional list of criteria must also be satisfied. Sensitive data are defined as those that consist of information as to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life and criminal offences. The list of criteria for processing sensitive data is restrictive. In very many cases the data subjects' explicit consent is required before such data are processed.

Notification: Data controllers are required to notify the supervisory authority of their processing operations for inclusion in a public register. Some exemptions exist. There is a fee for notification of £35 (approximately $50) per year. This indirectly funds the Information Commissioner's office.

Supervisory Authority: The Information Commissioner is the independent public supervisory authority with appropriate powers of investigation and intervention to monitor compliance with the law and hear claims lodged by individuals.

International Co-operation: Arrangements for co-operation between supervisory authorities in member states and the EU Commission are established. These include a working party of representatives of supervisory authorities (Article 29 Working Party).

Individual Rights

Access: Individuals have a right to know whether or not a data controller is processing data about them, a right of access to such data and a right to any available information as to their source. There are some limited exemptions from this right. A fee of up to £10 (approximately $15) can be charged and there are up to 40 days to respond. There is also a right to knowledge of the logic of any automated decision taking that the individual is subject to.

Correction/Deletion: There is a right to rectification, erasure or blocking of data which are incomplete or inaccurate.

Prevent Processing: Individuals have a right to object to the processing of personal data about them:

- where the processing causes substantial damage or substantial distress to an individual and that damage or distress in unwarranted or;
- where the processing is for direct marketing.

This right is further developed in the regulations implementing the Telecommunications DP Directive. Data subjects have a right to opt out of the receipt of unsolicited marketing calls through the telephone preference service and must not be sent marketing faxes without their consent

Automated Decisions: There is a right not to be subject to decisions that are taken solely by automated means and have a significant effect on the individual, for example in connection with assessing creditworthiness. A decision can be taken in the

course of entering a contract provided there are safeguards such as a right of appeal.

Request Assessment: The supervisory authority is required to hear claims lodged by any person concerning the processing of their personal data.

Compensation: Any person who suffers damage and associated distress as a result of a breach of the Act is entitled to compensation from the data controller. Claims must be pursued through the courts.

Data Protection Principles

These set out standards to be followed by data controllers in their processing of personal data.

Fair and Lawful Processing: As well as meeting the criteria for processing referred to above data controllers must process personal data in a way that is fair to individuals and does not lead to breaches of the law. In particular, to make processing fair, individuals should be made aware who is holding their data, the purposes of the processing and any other information necessary to make the processing fair such as the recipients or categories of recipients of the data. This obligation applies even where the data have not been obtained directly from the data subject, for example where they have been obtained from a credit bureau, unless providing the information would involve disproportionate effort.

Limitation of Purpose: Personal data must be collected for specific and lawful purposes and not processed in a way that is incompatible with those purposes.

Data Quality: Personal data must be:

- adequate, relevant and not excessive for the purpose for which they are collected;
- accurate and, where necessary, kept up to date;
- kept no longer than necessary.

Security: Data controllers must have appropriate technical and organisational measures in place to protect personal data. Where a data controller uses a processor to process data on its behalf there must be a contract in place tying the processor to only using the data in accordance with the controller's instructions and placing security obligations on the processor.

International Transfers: Transfers of personal data to countries outside the European Economic Area, so called "third countries", are only allowed if the country provides an adequate level of protection for the data. There are some exemptions that allow transfers to take place in circumstances where adequacy is not achieved.

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES

Adequacy

Whether a country provides an adequate level of protection for personal data does not depend solely on whether the country has a Data Protection law. The Act makes it clear that other factors must be taken into account including the nature of the data, purposes and duration of processing, the legal framework, codes of conduct or other enforceable rules and security measures. It is perfectly possible for example that a country might be considered adequate for the transfer of names and addresses on a mailing list but not for the transfer of medical records. The existence and effectiveness of any system of self-regulation is an important factor in assessing adequacy.

The Act gives effect to "Community findings". These are decisions of the European Commission that the level of protection in a third country is or is not adequate. There have been Community findings in relation to Switzerland and Hungary as well as the US safe habor arrangements. Several other countries are under consideration.

Exceptions

In limited circumstances transfers of personal data to third countries can take place even though adequacy has not been established. These are where:

- the data subject has consented to the transfer;
- the transfer is necessary for performance of a contract involving the data subject or in the interests of the data subject or for pre-contractual steps;
- the transfer is necessary for the reasons of substantial public interest;
- the transfer is necessary for legal proceedings, obtaining legal advice or otherwise for the establishment, exercise or defence of legal rights;
- the transfer is necessary to protect the vital interests of the data subject;
- the transfer is part of the information in a public register.

In addition transfers can be made on the basis of a contract between a UK data exporter and a data importer in a third country which is of a type approved by the Commissioner. The Commissioner also has the power to authorise particular trans-

fers on the grounds that they are made in such a manner as to ensure adequacy. The Commissioner has not yet given approval to any standard contract terms. She is awaiting the outcome of work the European Commission is undertaken to develop such terms which will then be subject to a Community finding.

ENFORCEMENT

In the UK, breaches of the Data Protection Act 1998 are mostly not criminal offences. The criminal offences are largely confined to failure to notify the Commissioner of processing operations requiring notification and knowingly or recklessly, without the consent of the data controller, disclosing or obtaining personal data. Within this the Commissioner places particular importance on using her powers to prosecute those who seek to obtain personal information, to which they are entitled, by deception.

Where there is a breach of one of the principles, the Commissioner can issue an enforcement notice requiring the data controller to take action to bring about compliance, for example, to delete data. Failure to comply with a notice is then a criminal offence. There is no power to "punish" a data controller for a breach of principles.

The Commissioner also has a power to issue an information notice requiring a data controller to provide her with information needed to determine whether there has been a breach of the Act. There is a right of appeal to an independent tribunal against enforcement or information notices. Where she has reasonable grounds for suspecting a breach of the Act she can apply to a court for a search warrant in order to obtain evidence.

In addition individuals can take their own cases to court. They can ask the court to:

- order a data controller to uphold their right of access, right to prevent processing and rights in relation to automated decisions;
- order a data controller to rectify, block, erase or destroy inaccurate data.

THE INFORMATION COMMISSIONER

The former Data Protection Commissioner has recently been renamed "Information Commissioner". This reflects additional responsibilities for oversight of the UK's new Freedom of Information Act. This testimony only addresses her responsibilities under the Data Protection Act 1998. She operates through an office with around 115 staff and a budget of £4.5 million ($7 million).

Duties

In addition to enforcement and maintenance of the public register of notifications the Commissioners functions under the Act include:

- promotion of good practice which is such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others and includes (but is not limited to) compliance with the requirements of the Act;
- dissemination of information and the provision of advice to individuals and data controllers about the operation of the Act, good practice etc;
- assessing, with the consent of the data controller, any processing of personal data for the following of good practice (an audit function).
- presentation of an annual report and, when she sees fit, other reports to Parliament;
- provision of assistance to individuals taking action through the courts in relation to the processing of personal data for journalism or for artistic or literary purposes;
- preparation and dissemination of codes of practice;
- determination of requests for assessment.

Codes of Practice

The Commissioner is required, after consultation, to prepare and disseminate codes of practice for guidance as to good practice either where she is directed by the Government to do so or where she considers it appropriate. Such codes explain the Commissioner's view of how compliance with the requirements of the Act should be achieved in practice in a particular field of business or activity. She can also encourage trade associations to prepare codes.

A code of practice has been issued on the use of closed circuit television in public places. Consultation has recently been completed on the draft of a code on the use of personal data in employer/employee relationships. The Commissioner places considerable emphasis on the development of codes of practice under the Act. She be-

lieves they have an important role in translating the necessarily general requirements of the Act itself into meaningful standards that can be readily applied in the context that they address.

Requests for Assessment

A request may be made to the Commissioner by a person directly affected for an assessment as to whether it is likely or unlikely that any processing has been carried out in accordance with the Act. Subject to some limitations the Commissioner is required to make an assessment and inform the person of the result. This replaces her duty under the Act's predecessor to consider complaints. In some cases requests for assessment may lead to enforcement action.

Around 5,000 cases are handled each year. Roughly half of these require some form of investigation. The others are dealt with by the provision of information or advice. Around 65% of cases reveal a breach of the Act. The two largest categories of cases in 1999/2000 were consumer credit (including credit reporting)—31% and direct marketing—18%.

Strategy

The Commissioner sees her role as wider than simply undertaking the specific functions given to her in the Act. Her mission statement commits her to promoting respect for the private lives of individuals and in particular for the privacy of their information by:

- implementing the Data Protection Act 1998 and;
- influencing national and international thinking on privacy and personal information.

She is concerned to ensure that data protection and privacy issues are identified and addressed at the inception of new laws, processes and systems. It is central to this that;

- those who handle information both in the public sector and in the private sector are aware of their obligations and act accordingly;
- data protection emerges as a feature of good business practice and is seen as a necessity for recruiting and retaining customers rather than as a regulatory burden;
- policy makers, particularly at governmental level give appropriate weight to individuals' privacy rights in the development of new legislation, international instruments, public policy and the delivery of services.

In addition the Commissioner seeks to develop a climate in which individuals are aware of their rights in relation to their information and feel confident that these rights are respected and can be exercised.

Some specific activities that the Commissioner is or has recently been involved in include:

- implementation of a national advertising campaign related to individuals' rights;
- development of education packs for use in schools;
- supporting the development of data protection qualifications and the incorporation of data protection material in other relevant syllabuses;
- preparation of guidance and materials to assist data controllers with compliance eg a data protection audit manual;
- encouraging the work of national and international standards bodies on data protection;
- development of design notes for systems developers to ensure that privacy protection is incorporated in standard design methodologies;
- promotion of a debate on current data protection and privacy issues through conferences/seminars;
- encouraging effective self regulatory initiatives that can operate within the legislative framework particularly in connection with e-commerce;
- supporting the development and use of alternative dispute resolution procedures for handling data protection complaints.

Recently the Commissioner has been invited to contribute to the UK Government's appraisal of the UK's new data protection regime. This has been conducted partly with an eye to the review of the EU Directive due by 24th October 2001. Many of the points raised in her submission are matters of detail but she draws attention to some areas where, in her view, the law imposes burdens on data controllers that are out of proportion to the benefit, if any, that they bring to individuals. These include:

- the application of the law to situations where a data controller is not established in the UK but nevertheless uses equipment in the UK for processing;

- the concept of special or sensitive categories of data rather a recognition that it is the circumstances in which personal data are processed that make them sensitive;
- the provisions on automated decisions;
- the extent of the notification obligation on data controllers;
- the emphasis placed in the provisions governing transfers to third countries on centralised decision making rather than leaving decisions and arrangements on adequacy to data controllers, in the first instance.

In addition the Commissioner has commented on some areas in which she considers the law could better protect individuals. These include:

- the lack of a right to compensation for distress caused by a breach of the Act when there is no associated damage;
- the restriction on her right to assess a data controller's processing of personal data for the following of good practice which means that she can only do so with their consent;
- the lack of a power to impose a penalty rather than merely ensure compliance where a data controller knowingly or recklessly breaches the Data Protection Principles.

FURTHER INFORMATION

The Commissioner would be pleased to supply further relevant information that the Sub-Committee might require.

Mr. STEARNS. Well, I thank you, Mr. Smith.

I will start with the questions here. Let me say to my colleagues, if you have a business in Europe, and you want to use the internet to send out information back to the home company in the United States, you have an option of complying with the European Union's privacy provisions, or you have an option of the safe harbor agreement that was worked out between the administration and the European Union.

Only 20 corporations, less than 20 corporations, have signed up for the safe harbor agreement, because it doesn't appear, at least from an American standpoint, to be practical. So a third alternative for you, if you are in Europe and you are doing business, and you want to send back information and do everything, is what is called a model contract.

And so the gentleman we have here, my colleagues, is head of what is called the Article 29 Working Party, which is all of the European Union representatives come together and talk about how they are going to develop these model contracts.

So the first question I would like to have for Professor Rodotà is, what are the key terms spelled out in these model contracts? Do U.S. companies have any room to negotiate the provisions? If so, with whom do they negotiate? The company wishing to transfer data or a privacy commissioner? Do you understand that, or is the question clear?

I think we need to know for American corporations, what are the key terms of the model contracts? Who do they negotiate, the company, or do they have to come to you as part of the privacy commissioner?

Mr. RODOTÀ. No. No. The companies does not have to come to the Data Protection Authority. Now the standard contractual clauses have been approved by our group, and now they are on the way to be approved by the Commission.

So when this kind of model contracts will be approved, both parties—the exporter and the importer, the European part and the U.S. or the third country part, can pass a contract without an intervention of the Data Protection Authority at the European

level, because it means that they are using a contract sealed by the European Commission.

So if they respect the terms of the contract, they have a mechanism, an instrument, giving them the opportunity to comply with the adequacy test. This is a traditional contract. Yes, I don't know if my answer——

Mr. STEARNS. Can they negotiate terms?

Mr. RODOTÀ. Partly. Partly.

Mr. STEARNS. Partly.

Mr. RODOTÀ. You have the model contract, a model contract, the possibility to choose some options, yes, especially on the side of the enforcement, because you can have the possibility of—I have here the text of the—yes, the model contract.

You have the possibility to, for instance, in the part of the obligation, to choose the legislation of reference, the different—the mediation and jurisdiction for possibility for solving the conflicts. So they are part—they cannot make us see it—the part referring to basic principles of the directive. And other parts parties can have the possibility to choose.

Mr. STEARNS. Mr. Smith, your testimony states that the Office of Information Commissioner has "appropriate powers of investigation and intervention to monitor compliance with the law." Could you explain the limits of those powers? Could you please provide us with any examples of the application of said powers the Information Commissioner has taken to date for possible violation of the law?

Mr. SMITH. Yes, Chairman. There are certain criminal offenses, as I mentioned, under the Act—obtaining information by deception. We have prosecuted a number of organizations and individuals for that. We also prosecute for failing to be registered or notified with our authority.

Where there are more matters that require investigation, whether they are criminal matters or breaches of the Data Protection Principles, we have powers to obtain search warrants, and we go before the court and obtain a search warrant to obtain evidence, and we have done that on several occasions.

We also, under the new law, have a power to issue information notices which require businesses to answer questions which are necessary for our investigation. We have yet to use that, because this has only just come into being. And our powers then are—for general breaches of the Act are to issue enforcement notices, which require a business to change its practice to delete data, to provide notice and choice, or whatever.

We have used that on probably about a dozen occasions up to now and—those cases, and some of them have gone to an appeal tribunal, which has generally found in our favor.

Mr. STEARNS. Thank you. My time has expired.

Mr. Towns, ranking member?

Mr. TOWNS. Thank you very much, Mr. Chairman.

Mr. Smith, has the EU or any member country taken action against a firm for its failure to comply with the requirements of the privacy directive? And, if so, has any EU firm been forced to seize data operations as a result of the non-compliance?

Mr. SMITH. I can only answer in relation to the United Kingdom. We have taken action—because of the privacy directive, the law implementing that has only very recently come into force. The action we have taken under that, although there have been—we have commenced proceedings, in a number of cases is limited, but our old law was very similar and there were cases under the old law.

We have required businesses to stop using information in the way that they were using it previously, and in some cases they have had to change their practices significantly. One recently has been in relation to utility companies, which were privatized, and the use of information for marketing purposes fall in privatization. And they have had to revise significantly their practices as a result of our action.

There are others I could give, but we have required changes, certainly.

Mr. TOWNS. Thank you. On that note, well, are the privacy contracts that are negotiated with foreign firms reviewed by EU officials, or is each country's privacy director responsible for determining that the contracts are consistent with the privacy directive? I mean, who makes that decision?

Mr. SMITH. Under the UK law, which is not necessarily identical to the laws of every member state, there are two ways. One is the way Professor Rodotà has described, which is that there are model contract clauses approved by the Commission, and when those are approved UK businesses are perfectly entitled, and we would encourage them to use those and rely on those.

There are also arrangements under the law where we, as Commissioner, can approve model contracts or individual arrangements between one company and another. And at the end of the day, the UK law requires adequacy, and it talks about adequacy being assessed on the basis of arrangements that apply in a particular case, whether—including terms such as codes which apply in general or in a particular case.

And a contract is an enforceable arrangement that applies in a particular case. So it is possible for a UK business to develop a contract with a U.S. business, which does not necessarily follow precisely the model, if it is eventually approved by the community, and still ensure adequacy.

So it is possible for contracts to be developed and to meet the requirements of the law.

Mr. TOWNS. All right. Go ahead, Professor. Yes?

Mr. RODOTÀ. Yes. Let me describe very precisely a situation that can occur in all member states of the European Union. Because until now there are many cases in which the data protection authorities were asked by European and U.S. companies to agree with their contract.

They control if they submit to the adequacy test, the contract submitted by both parties, and they are mostly in Germany. A very important contract passed by U.S. Citibank and Deutch—and the Deutch Railway. And in other countries like France, Spain, Italy, there are many cases in which until now not having some general rules like safe harbor, and not model contract approved at the European level, they used the possibility to ask in specific cases the data protection authorities.

This is a very well-established procedure. Not easy. Not easy.

Mr. TOWNS. Right.

Mr. RODOTÀ. Very, very bad for the data protection authorities.

Mr. TOWNS. Are these private contracts disclosed publicly?

Mr. RODOTÀ. Yes. They are always brought to the Data Protection Authority.

Mr. TOWNS. Well, how could I get one? How do you get a copy of them? How do people get copies of them?

Mr. STEARNS. He would like to get a copy himself.

Mr. SMITH. Certainly. The individual contracts would not be made publicly available. The only contracts which may be publicly available are the model which has been referred to.

Mr. TOWNS. So, I mean, that is secret. Okay. Well, anyway, let me move on. You have been traveling a great distance.

Let me just ask one other question, Mr. Chairman.

There was a survey conducted by the Kearny Management Group which was reported in November of last year in the publication "Biz Report"—confirms this point. Let me quote, "E retailers worldwide lose $6.1 billion"—that is B as in boy—"in sales due to an 80 percent failure rate among online purchase attempts, and that invasive information requests are blamed for 52 percent of sales that fall apart, followed by reluctance to enter credit cards, 46 percent." Do you agree that business is paying a big price for the confidence consumer lacks in the privacy security of their online transactions?

Mr. SMITH. Yes, we would agree that there is a real problem there and that those businesses that recognize the true situation actually build privacy into their practices as a way of attracting and recruiting, keeping customers, rather than simply as a regulatory requirement.

Your figures are supported by a whole range of studies, and our perception in the UK is the same as yours. Businesses increasingly will—not increasingly, but we do find businesses that adopt practices online which, in our view, are not acceptable and do not necessarily comply with the law, particularly excessive information gathering, requiring information as a condition of doing business where that is not necessary for the transaction, and failing to provide the choice that is allowed, and operating in an underhand way, not giving notice of information collection practices which are taking place through the use of cookies and mechanisms such as that.

Mr. TOWNS. Thank you, Mr. Smith.

Thank you, Mr. Chairman, for your generosity.

Mr. STEARNS. The gentleman's time has expired.

Mr. Shimkus is recognized for 5 minutes.

Mr. SHIMKUS. Thank you, Mr. Chairman. Mr. Chairman, I would recommend that also the OECD was mentioned in some of the opening statements. I had a chance to visit the OECD on the NATO trip. A lot of people—we don't—a lot of us don't know what that is, but we are a member. And we have an ambassador and a staff, and if they are doing issues on privacy we should probably call them to see what our response is in that organization, and I would be willing to help facilitate that.

Mr. STEARNS. It is a good idea to coordinate with them, too. Yes.

Mr. SHIMKUS. Because they are working in conjunction with our European allies, not just—Mexico is a member, Korea is a member. It is a pretty big international grouping of nation states.

Mr. Smith, I would like to—you also mentioned effective remedies for individuals, dispute resolution, which implies that there will be some information that will be improperly used, and that individuals will try to address redress, or get redress, which brings up the issue that I would like to ask on is the Investigative Powers Act or the RIP Act, which, again, based upon my opening statement, privacy is the utmost issue we had to debate here in our country on the CARNIVORE issue.

The fact of being able to gather all of the communications, hold them in a bank of information for 7 years, and require people who are doing business to do so, I think is really a threat on privacy issues for our companies and individuals.

And I would like to follow up with a question to both of you is, Professor Rodotà, how does the EU Data Privacy Directive affect the RIP Act or similar laws that may pass in other EU countries? And how would the EU directive protect non-EU members from the UK government storing personal information about them?

Mr. SMITH. Perhaps if I start, and then Professor Rodotà can take up the general European situation.

Mr. SHIMKUS. Great.

Mr. SMITH. The RIP Act, the Regulation of Investigatory Powers Act, doesn't actually include any measures that require or necessarily permit businesses to store data solely for—or telecommunications providers solely to store data——

Mr. SHIMKUS. No. But the government stores it.

Mr. SMITH. Well, no, not under the Regulation of Investigatory Powers Act. The Regulation of Investigatory Powers Act only gives powers of interception, and we, as Commissioner, expressed views which weren't necessarily taken into account in the final version.

You are quite right that there are proposals or suggestions to retain data for investigatory purposes. They are not actually part of the RIP Act, and they haven't yet been brought in. The suggestion of 7 years is merely in a leaked report from the National Criminal Intelligence Service and is by no means government policy.

Government policy, as far as we know at the moment, is not to legislate in this area and to wait until international instruments address the matter and essentially set the standard.

So I think there may be some misunderstanding. There is no requirement at the present time to keep traffic data for investigatory purposes for 7 years. We would be very much against that. If there is to be a period of retention at all, it should be very much shorter than that. And as I say, it is a matter being addressed by international instruments, which is what Professor Rodotà——

Mr. SHIMKUS. But if I may, before we go to the EU aspect, but is there—okay. If it is not a collection, is there a review of all data coming in, electronic, internet, or cell, or land line review, under the RIP Act?

Mr. SMITH. No, there isn't. I mean, there are arrangements whereby interception can take place. Essentially, there are provisions. They have to be authorized by—in some cases by the Home Secretary, in other cases by a senior police officer or equivalent.

And one of our concerns when the bill was going through Parliament was the level of that authorization. We asked for it to be higher than it is. But there is an arrangement whereby interception does have to be authorized on a case-by-case basis.

Mr. SHIMKUS. We had this debate on the encryption debate and law enforcement. It got very contentious here.

And I will finish up with, if I may, Mr. Chairman, allowing the Professor to finish, and that will end my time.

Mr. RODOTÀ. I would like only to say that this problem is now under discussion in Europe, because the way in which traffic data can be collected is under discussion in the framework of the Council of Europe Directive on Conventions on cyber crime. And also, the U.S. are part in the negotiations.

Generally speaking, the attitude is different in different countries. But the work—the Article 29 Working Party passed the resolution last year, very clear on this point, saying, first of all, that no interception can be made without an authorization by jurisdictions. And no collection, massive kind of data collection.

This is the problem—two very important principles in the directive are: first of all, the principle of finality; and, second, the principle of proportionality. We were, and we are, strongly against any kind of massive collection, without the specific and indicated aim. We are asking also for a very short period in the duration for this kind of collection of data. They are moving in different directions.

For instance, the Belgium Parliament has passed, for security reasons, for the first time, a law saying that data can be stored for 1 year, and that they are going beyond the indication Article 29, saying they were much more in favor of shortest time of conservation.

Mr. STEARNS. The gentleman's time has expired.

Mr. Gordon, the gentleman from Tennessee, is recognized for 5 minutes.

Mr. GORDON. Mr. Shaw, if I could follow up on some comments you made earlier. You were talking about how individuals in the United Kingdom had the right to go to court, if necessary, to protect their rights if—as individuals. Do you have what we would call class action lawsuits here? Do they go as an individual, or can they bring in large groups of individuals that they feel are in that same situation?

Mr. SMITH. No, the UK law, as it stands at the moment, only allows individuals to bring cases. And I think it is fair to point out that actually the individual's rights are fairly limited, and that it only enables them in terms of getting redress, to get compensation for damage, which in UK legal terms involves some sort of financially quantifiable loss. And most of the data protection breaches result in distress to individuals, but not necessarily a financially quantifiable loss.

So I think we have been asked, as Commissioner, to express our views on the law, and it is one area we feel the law could be improved in providing redress for individuals.

Mr. GORDON. So if you are a U.S. company thinking about doing business in Great Britain, I guess my thoughts would be, certainly, if I was looking at Europe at large, that although United Kingdom has not opted into the Euro, it would—you know, certainly, the EU

is trying to bring down barriers among their own countries and trying to become more productive in terms of their commerce there.

But this is—I guess in Tennessee we would call it a little looseygoosey. I mean, you know, if I am a company, and I am trying to do business in Italy and maybe in France, and a couple of other countries, under a safe harbor I would be somewhat concerned that maybe one country would say okay, another country maybe not. You know, it makes you concerned there.

So if you are deemed not properly within the safe harbor, what are the penalties? What risk does an American company, Mr. Shaw, risk?

Mr. SMITH. If a company is not part of the safe harbor and transfers——

Mr. GORDON. Or tries to be, but deemed not so.

Mr. SMITH. Yes.

Mr. GORDON. In one—say, potentially, two countries say yes, but another country says no.

Mr. SMITH. Yes. I mean, that is not how the safe harbor works. It is up to the U.S.—I believe it is through the Federal Trade Commission—to take people onto the safe harbor list. And if they are taken onto the list, then we and all of the other EU member states have to recognize them as providing adequate protection. We have no choice in that, and this is a common standard.

The area where penalties would come in is if a U.S. business is not in a safe harbor, has made no arrangements for adequacy, has no contract or other arrangements, and is transferring data in breach of the law. And then our power would essentially be to provide them with an order to stop them transferring that data. And if they failed to comply with that order, then they could be prosecuted for a criminal offense.

Mr. GORDON. Okay. So if the FTC says that they are in compliance with safe harbor, but, again, a country in Europe disagrees with that, then does the FTC's position trump it?

Mr. RODOTÀ. I would like to—also to go back to the first—the first question you raised. In Italy, we have no class actions, but there is the possibility, if the people make this kind of decision, to be assisted or to be substituted by a tribunal or organization.

In the situation of a weakness or the part asking for the respect of the law, the individual can give the possibility to a group to act in—on behalf on its own interest. This is very interesting machinery.

Second, the problem if this—there is the possibility that the same request made by a U.S. company in France or in Italy have different answers. It is possible that they can escape this risk using one or two means. There you have safe harbor or standard contractual clauses.

Third, if there are the possibility—if some data are transferred without entering the safe harbor, without having—using model contract, without previous authorization of the national Data Protection Authority, they are in infringement of law, surely, for the national authority.

What happens if there is a discrepancy between what the FTC decides and the attitude of the national Data Protection Authority?

That is a problem. That is a problem because we are waiting for the way in which the Federal Trade Commission will——

Mr. GORDON. Excuse me. We have a limited amount of time. So, again, so you are saying, then, that there can be a situation where the FTC could grant safe harbor, but an individual European country could say, "We don't agree with that." Is that——

Mr. RODOTÀ. They don't agree with the safe harbor——

Mr. GORDON. All right. So, then——

Mr. RODOTÀ. [continuing] with the FTC decision.

Mr. GORDON. All right. That is not consistent, then, with what Mr. Shaw said, is it? And I am trying to figure out—Mr. Shaw, is that——

Mr. STEARNS. Mr. Smith, you mean.

Mr. GORDON. Mr. Smith. I am sorry. Excuse me. Is that—that sounds to be inconsistent there with your statement. Is that true or not? I am just trying to—I am not trying to get a fight here. I am just trying to find out what is going on, and then trying to see what level of risk our countries are taking, or our companies are taking.

Mr. SMITH. My understanding is that if a business is on the safe harbor list, we, as a supervisory authority in the UK, cannot act to stop transfer to that business, unless there is some breach of UK law taking place in the UK prior to transfer, which, you know, would be the same as if the transfer was to a company in France or even to another company in the UK.

The only area where I believe we could take action is if the company has failed to comply, demonstrably failed to comply with the safe harbor arrangements, and then the—and no action has been taken. But, essentially, if they are on the safe harbor list, then they are approved in that sense.

Mr. STEARNS. The gentleman's time has——

Mr. GORDON. Yes. But you are still the final arbitrator of that.

Mr. STEARNS. The gentleman's time has expired.

Let me just, have you folks finished your answers? Yes.

The gentleman from New Hampshire, Mr. Bass, is recognized. He is not here.

Then, Mr. Doyle is recognized.

Mr. DOYLE. Thank you, Mr. Chairman.

You were asked earlier, I believe, by Mr. Towns about the privacy contracts and whether they were disclosed publicly, and I believe your answer was that they weren't, that they were private, is that correct?

Mr. SMITH. Yes.

Mr. DOYLE. So when a company negotiates a private contract with the privacy director, that is only known—the details of that are known between the company and the privacy director. Yet when companies go the safe harbor route, the details of that agreement are posted on the internet and are publicly disclosed for all to see.

Do you think maybe that explains why so few companies go the safe harbor route? Wouldn't it be smarter for them to make their arrangements with the privacy director in private without disclosure? How does one police—you know, if the contracts are private, you know, how does one know what agreements are being made in

private between the companies and the privacy director, as opposed to companies that go the safe harbor route and disclose everything?

Mr. RODOTÀ. That is a matter of the politics of each company. But generally speaking, I think that entering safe harbor means the company can transfer data by European partners without any specific and case-by-case procedure. Otherwise, in any case and for every counterpart you have in Europe you must engage a specific procedure before the national Data Protection Authority.

I think that the economy of means may be balanced by the limited publicity of——

Mr. DOYLE. So if you are dealing in multiple countries, you would have to get a separate contract in each one of these countries. And that hassle, or, you know, whatever that would entail is outweighed by the disclosure.

Mr. Smith, do you agree with that?

Mr. SMITH. Yes.

Mr. DOYLE. Let me ask you another question. Do you think the European Union privacy directive, do you think it was a reactive initiative and measure? That is, that European industries weren't practicing self-regulation and the government needed to step in and put an extra level of protection, or do you simply see it as something that complemented what industry in Europe was doing?

Mr. SMITH. Yes. I think the thinking behind the directive was from a slightly different perspective. It was essentially seen as the development of the single market within Europe. And in order to remove the possibility of, say, the UK businesses not being allowed to transfer data to France, for example, on the basis that there was inadequate protection, the directive would bring all countries up to a roughly similar level. So there is no basis for restricting the flow of data.

I think that was the thinking behind it. I mean, in most countries, but not all, there was data protection law beforehand. There was in the UK. And I think the roots of that were primarily in the human rights argument that there needed to be a level of protection. We had signed up, as the UK, to the Council of Europe Convention and should have had a law, then, to implement that.

But also, as I mentioned earlier, there was a strong lobby in the UK from the business community, from the Confederation of British Industry, to have data protection law in the UK, firstly, to give some reassurance to consumers that they could trust companies which computerize their data—was basically the position at that time. But also, to bring the UK at that time into the European data protection, if you like, club, to enable it to participate in the flow of data.

So I don't think there was a great deal of look at, if you like, whether self-regulation was effective or not in terms of developing the law. But what we are seeking to do now is very much encourage self-regulation and self-regulation to resolve, if you like, day-to-day consumers' problems and individuals' problems but with a backstop of the law. So if that fails, then the law is there to provide the final area.

Mr. DOYLE. Just one last question. To the four countries, Professor, that you said were in non-compliance with the directive—Germany, France, Ireland, and Luxembourg—are the data firms in

these countries being forced to enter into privacy contracts to continue transfers with other EU members?

Mr. RODOTÀ. The fact that they have not implemented the directive does not mean that they have no data protection. They have data protection. France and Germany have very well-established, since 1978, data protection laws. They have Data Protection Authority very, very prominent in France and in Germany. In Germany, they have also the Federal level. It means that they have data protection authorities in every land. So I think that that is not a problem.

I would add a word on the problem of industry, self-regulation, and the framework of directive. I think that we are now assisting to a very interesting development inside Europe, because the codes of conducts are not at all considered as an expression of a specific sector. You know that there is an article in the directive, the Article 27, implementing the codes of conduct.

This means that the interested sector can submit a draft to the workgroup—Article 29 working group—asking for a seal, in brackets, for a seal. And it means that this kind of codes of conduct comply with the general principles of directive. Expression of a representative sector of the industry are agreed, and they have not only a moral suasion, much moral suasion, but they can better be implemented also at the code level. It is very important.

And, in Italy, we are now developing this experience of codes of conduct with different sectors. Media, it is working very well; the sector of research, historical statistics; the sector of private investigation; banking and insurance now we are underway.

It is very important, because we have a general set of legal established principles and a tool, the codes of conduct, for making these principles flexible. This is very important. But it means that you have at the national level, or the European level, one single body giving this kind of seal.

And if I can express an opinion, it would be very important for all of the world if also United States will have an agency, a privacy agency, giving this opportunity to the citizens and also to the business community.

Mr. DOYLE. Thank you.

Mr. STEARNS. The gentleman's time has expired.

Mr. Buyer is recognized for 5 minutes.

Mr. BUYER. I want to thank you, Mr. Chairman, and I want to thank the witnesses for coming. I want to make a few comments, and then I want to solicit your response to my comments and my question.

I have been upon the European continent. Not only as a private citizen, but I have worn the uniform, and as a Member of Congress. One thing I enjoy are these discussions, because it always reinforces what I believe was good judgment of my ancestors to leave the continent.

Okay? I find myself troubled at the moment. I am troubled because, as I watch the European Union sort of try to come together, which in world history is amazing. Because you mocked us at the creation of our country, as we were called the Grand American Experiment. Perhaps we can now look back across the ocean and sort of mock you back and say, "Well, let us see if it can succeed."

And then, I find myself here in Congress, and say, "Well, I do agree in a quest for economic harmony?" That is what we are trying to do as each of us, as sovereign nations, seek to protect our own identity, and how we choose to recognize rights and govern. Okay?

You, meaning the European Union, and those member countries, have chosen to give up something for some social compact. Am I now here in this country supposed to accept that your model should be the standard for the world? I am bothered and troubled at the moment.

I find myself a few years ago having to vote on some measures here in Congress that were negotiated with countries around the world, or whether we should create the World Trade Organization and The General Agreement on Tariffs and Trades. It was very difficult to get Europe to agree on certain things. So in the end, in order to get signatures, we created carveouts and exceptions.

Now I find myself troubled and ask, are these carveouts and exceptions being exploited? We recognize that nations want to protect, certain things, whether it is cultural or other types of things. Like, are we are not going to let those genetically engineered organisms come in upon our continent? My gosh, let us just prevent all that U.S. agriculture from coming in. So they exploit an exception.

So I am curious as I sit here, because you are the experts now. What protections did the EU nations make to ensure that the data protection did not generate a violation of the commitments that your nations made to the World Trade Organization? Do you believe that it did or did not? I am interested in the response from both of you.

Mr. RODOTÀ. I emphasized at the beginning of my statement that there is an important evolution in the European Union, giving an important protection to personal data because they are considered a very important part of fundamental human rights. And if we are living in the information society, information about individuals becomes more and more important for respecting the individual rights.

There is not an idea to impose a model to the world or to defend a cultural identity. Europe accepted the modern idea of privacy protection coming from the United States. That was very important for us. We recognized a very important improvement in the idea of democratic rights, privacy. We accepted this idea. And as a very prominent law philosopher, Ronald Dworkin, teaching in the U.S. said, we have taken rights seriously.

So at this very moment, we are not trying to impose our model. We are trying to have a dialog on these very important issues with all countries, and we respect the idea and the model of U.S. Otherwise, the safe harbor could not be possible.

But at the same time, we have considered privacy problems according to the very, very long American tradition. I am a professor of law. I know very well the seminal work of Warren Brandeis published in the Harvard Law Review in 19—at the end of the 19th century, 1890, in the Harvard Law Review.

And the idea of privacy was not directly connected with economic at first. We must have a balance. This is our attitude, and I think that we can have a fruitful dialog on these points.

Mr. SMITH. I have nothing to add.

Mr. STEARNS. The gentleman's time has expired.

Ms. DeGette is recognized for 5 minutes.

Ms. DEGETTE. Mr. Chairman, thank you very much. And I wasn't here at the beginning of the hearing, I was on the floor, and so I would like to ask unanimous consent for myself and all other members to submit their opening statements for the record, Mr. Chairman.

Mr. STEARNS. Unanimous consent so granted.

Ms. DEGETTE. Thank you. And I am sure that my colleagues thanked both of you for traveling here to testify today, but I would like to add my thanks. I know that the European Union has tried very hard to craft a policy directive that will protect consumers and at the same time encourage commerce.

And I, for one, think that it is a noble effort, and I am sure that most of the members of this subcommittee would share my congratulations. As with the United States, it is an evolving effort because of the evolving technologies. And I would just like to ask you gentlemen a couple of questions in that direction.

First of all, for clarification, Germany, France, Ireland, and Luxembourg, it is not that they are in non-compliance, in my understanding, it is that they have not yet adopted the EU Data Protection Directive. Would that be correct, Professor?

Mr. RODOTÀ. Yes.

Ms. DEGETTE. And I would assume in those situations that would be because they feel that they have their own laws which will protect privacy. I think you talked in particular about France and perhaps Germany.

Mr. RODOTÀ. No. I think that the reasons why they have not yet implemented the directive are political ones——

Ms. DEGETTE. I see.

Mr. RODOTÀ. [continuing] because they changed their majority, and the new government in France started again with——

Ms. DEGETTE. Okay.

Mr. RODOTÀ. I think that—and Germany is now trying to have a more comprehensive——

Ms. DEGETTE. I see.

Mr. RODOTÀ. [continuing] law than the——

Ms. DEGETTE. Then the——

Mr. RODOTÀ. [continuing] same directive.

Ms. DEGETTE. Okay.

Mr. RODOTÀ. I think that at the end of this year they will comply with that.

Ms. DEGETTE. They will. Now, I am sure both of you gentlemen are familiar with a recent study that was done by Consumers International. It was quoted extensively in The Wall Street Journal. And in the article, Anna Fiedler, who is the Director of Consumers International, said that the evidence shows there is a real lack of enforcement by the EU privacy regulations. So that even though they are on the books, they are rendered useless.

What is your opinion? Let us start with Mr. Smith, and then we will go to you, Professor, on that.

Mr. SMITH. Yes. Thank you. We have some—I mean, I have some sympathy with the article, although I think it perhaps goes a little

too far in saying that enforcement is useless. I mean, I have described I hope to the committee some of our enforcement action and the powers that we have and that we have used them.

But we have never seen formal enforcement as the primary mechanism of achieving data protection compliance. It is rather through a process of education, development, and encouragement, and developing it into good business practice, self-regulatory requirements, that compliance is being delivered.

Now, there is a long way to go, and the survey relates particularly to the world of electronic commerce——

Ms. DEGETTE. Right.

Mr. SMITH. [continuing] where there are real challenges.

Ms. DEGETTE. Thank you.

Professor?

Mr. RODOTÀ. Well, I think that—I know the study. I have seen the article in The Wall Street Journal. I am convinced that it is a misunderstanding. And they—this research gives a false impression of the real situation. They say 60 percent, if I remember correctly, of the American websites have——

Ms. DEGETTE. Privacy.

Mr. RODOTÀ. [continuing] privacy problem.

Ms. DEGETTE. Right.

Mr. RODOTÀ. And only 32 percent of the European websites have a privacy problem. But, in Europe, even if there is no policy indicated by the websites, in any case that is the law.

Ms. DEGETTE. Well——

Mr. RODOTÀ. And the citizens have the opportunity to use law without any reference to the politics indicated by the websites.

Ms. DEGETTE. Yes. But, Professor, what the study said was that more than 69 percent of European websites collect information by users, but only 32 percent point them to the privacy policy. What they pointed out is there is a lack of consumer confidence.

Mr. RODOTÀ. No. But——

Ms. DEGETTE. That is not correct?

Mr. RODOTÀ. This is—that is a problem. Frankly speaking, I must say that we are discussing the Article 29 group on the basis of a proposal of the French Data Protection Authority. The French Data Protection Authority make an inquiry in France for having the—for checking the kind of politics of privacy politics by the different websites.

And now we are discussing European level, in order to give also a European seal to the websites. But in any case, it does not mean that consumers in Europe have not enough protection. For instance, in Italy, some consumers ask our Data Protection Authority against some collectors of data, and we have the means to intervene. We intervened. We are the enquirer. And at the end, also we apply the sanction, and there is the possibility of an intervention of the judiciary.

And generally speaking, we have at the European level a recommendation of the Article 29 group saying that the invisible treatment, for instance through cookies, are in Europe completely illegal on the basis of the European directive.

Ms. DEGETTE. Thank you.

Mr. STEARNS. The gentlelady's time has expired.

Mr. Walden, the gentleman from Oregon, is recognized for 5 minutes.

Mr. WALDEN. Thank you, Mr. Chairman.

I appreciate your testimony today and your willingness to come here and share your views on the privacy directive and help us understand it better.

I am curious, given what you are trying to do to solve the problems within the EU countries, so you have a common threshold for privacy protection, when we look at those and say we have to comply in order to have commerce, in effect, what do we do when Canada or Argentina or somebody comes in with a different set of directives?

How is the EU going to relate to that if Canada, for example, has a different requirement than what you have negotiated with the EU? Is each country going to negotiate, then, separately with Canada or the U.S.? How does that work? Can either of you speculate on that?

Mr. SMITH. Yes. The European directive under UK law requires adequacy, not equivalence. It doesn't have to be the same as the directive.

Mr. WALDEN. All right.

Mr. SMITH. And, indeed, the safe harbor arrangements do differ from the directive. The Canadian law which is on the way to being approved, but has not yet been approved, is also significantly different. I mean, I do take your point that, you know, where you go to is sort of, when you do these comparisons, around the world. But with that approach to adequacy rather than equivalence, it shouldn't be too difficult to reach that sort of settlement.

We would also favor—I mean, it is not for us to put it forward. We are only the supervisory authority.

Mr. WALDEN. Right.

Mr. SMITH. Increasing development of international instruments, and the work which has been referred to as the OECD is particularly important in this area. And we would very much encourage it. I mean, that clearly would be the ideal, an international framework which we could all sign up to, which will provide the privacy protection effectively, and what is, you know, now a global market, where it is difficult to apply some of the nationally based regulatory requirements.

Mr. WALDEN. Because it seems to me—see if you agree with this—that your privacy directive, first of all, has an individual right of action. Somebody can sue, correct? And so one of the concerns I have, and I think shared by Mr. Buyer and others, is how that affects our sovereignty as a nation.

Because, in effect, you could export an enforceable legal right to the United States that could be litigated here by both an American and a non-American in our court system, in effect a law we have never voted on, enacted, and yet somebody can be sued here. Correct? I mean, that is what I am hearing is a possibility. Is that——

Mr. SMITH. I am not sure that I am in a position to answer that.

Mr. WALDEN. Okay.

Mr. SMITH. I think that is a question which really has to be directed to the European Commission rather than to——

Mr. WALDEN. I see. But do you see where we are headed here? Do you share that concern? What if we have one that could be litigated in the European Union without you ever having an opportunity to weigh in on it, if we pass a directive?

Mr. STEARNS. Just a point of information. I think the gentlemen, if they don't sign the safe harbor, they can't be prosecuted in the United States. But if they sign the safe harbor, and ultimately the model directive, yes, they can be sued.

Mr. WALDEN. But the impact, though, Mr. Chairman, is if they don't sign or don't agree——

Mr. STEARNS. Right.

Mr. WALDEN. [continuing] they have been excluded from commerce, so by de facto you either are excluded from trade or you agree to absorb somebody else's laws and suffer personal right of——

Mr. SMITH. I mean, that is certainly not how we as a supervisory authority would view it. I mean, those are——

Mr. WALDEN. Okay.

Mr. SMITH. [continuing] wide questions. But the simple approach that we would take is that if it is data on a UK citizen, that ought to be protected. And if that citizen gives the data to a business operating in the UK, that person ought to have some privacy protection. And if that company simply exports the data, not necessarily to the United States, to anywhere in the world——

Mr. WALDEN. Sure.

Mr. SMITH. [continuing] which doesn't have protection, that citizen is at risk, and increasingly so because of global markets and the internet and the way in which information can be moved around the world so readily. And it is simply a question of providing protection.

I think that does raise questions of the sort that you have raised, but those would not be, certainly from our point of view, at the top of the list.

Mr. WALDEN. Right.

Mr. SMITH. They are consequences rather than intentions.

Mr. WALDEN. I guess the problem—my time has expired, but I guess the problem I see is that, you know, okay, so we line up with the EU, and then, you know, China comes up with a different set, and then this is a pretty sticky wicket we are headed into. So I—I am out of time. Thank you.

Mr. TOWNS. The gentleman's time has expired.

The gentleman from Georgia, the ranking member, Mr. Nathan Deal? Actually, he is the vice chairman of the subcommittee, not ranking member, vice chairman.

Mr. DEAL. Thank you, Mr. Chairman.

And I would like to also express my appreciation to the panel members for coming and appearing here today. And even though I share with my colleague, Mr. Buyer, the thankfulness that my forefathers decided to come to this country and leave the continent, my forefathers from the south also went a little further and decided they didn't like the United States either and tried to secede from that.

And I must tell you gentlemen that we appreciate your—both your English dialect and your Italian dialect, as you speak the

English language. I must tell you, I hear with a southern accent, and I appreciate your efforts, and I will do the best to do my part as well.

In the discussion we have had, it is obvious that one of the concerns that we have as a Congress, and I think as individuals, is this issue of sovereignty. How do we deal with a directive that has now been adopted by 11, as I understand, of the European Union nations? And how do we incorporate that into what we do legislatively?

I think I understand the process that you have set up with the safe harbor and the contract approach, but I suppose the most important question that I would have at this point is our most recent attempts to legislate in the area of privacy related to financial institutions, commonly referred to—I believe we call it the Gramm-Leach-Bliley legislative initiative on financial institutions setting standards for privacy.

And I apologize if you have answered this question before I arrived. But it is my understanding that there has been a determination by the EU that these do not meet the standards of adequacy. Is that correct, or has there been any determination in that regard?

Mr. SMITH. I will explain my understanding, and Professor Rodotà can correct me if I get it wrong. My understanding is that there has been no determination. That in the course of the safe harbor discussions the question of the Gramm-Leach-Bliley legislation was put to one side and said we would look at that later, but it has not been returned to.

I am not familiar with all of the detail of it, so I can't give an authoritative answer. But I have been asked about it by UK financial institutions, and the view that I have expressed there is that it is, if you like, very good as far as it goes. It does—or it looks on the face of it as though it would provide adequacy in terms of notice and possibly choice, and it deals with security aspects.

But there are other issues that arise out of the European directive in the UK law to do with information being accurate, up to date, not kept for longer than is necessary, which I am not sure—and I only say I am not sure—I am not sure that the legislation necessarily addresses.

And, in fact, in terms of international transfers, the area it addresses most comprehensively, the notice and choice, is not necessarily a very big issue for—as in Europe, because essentially we are talking about data that have been collected already in Europe. So the notice and choice provisions are already there under European and UK law.

So those are only views off the top of my head from what I have looked at. It is not that there is anything wrong with what is there. It is not that it doesn't necessarily go as far as it should.

And I think, you know, concerns have been expressed about trying to export European requirements. I mean, the safe harbor arrangements are viewed as adequate. They are a U.S. approach. They are based on your self-regulatory arrangements. They are not the same as the European approach, but they have been viewed as adequate.

And although we are not trying to convince you to our approach, it is not our job to do that, it is simply to provide some information.

Some things it is hard to see in any, if you like, data protection or privacy system, how you can get away from some of the basics which I would hope we would all agree on, that information must be kept secure, people should be given notice, they should be given choice.

We might disagree about quite what that choice is and whether it is opt-in or opt-out. but for a very large amount of what we talked about, we must surely be agreed on what the basic principles are.

Mr. DEAL. Just very quickly before my time expires. In our dialogs and as go forward with consideration of privacy legislation in this country, we are concerned, as Mr. Walden has indicated, with the countervailing part, with the rights. We are trying to define rights of privacy, but we recognize that with every right there also must be a remedy.

And our concern with the litigation portion of it is we are a more litigious society than perhaps your continent is, and we are concerned about that and have to be concerned about it. So when we express those opinions, it is because of our own history with regard to when we define rights, and we provide remedies. Sometimes the remedies define the rights.

Mr. SMITH. Yes, we recognize that.

Mr. STEARNS. I thank my colleague. His time has expired.

We have finished with the first panel. Professor Rodotà, we thank you very much for participating, and Mr. Smith. We are delighted that the two of you took the time, and we hope you will stay around and listen to panel No. 2.

And with that, we are going to proceed forward here for another 15 to 20 minutes, and then we are going to break for lunch.

Yes?

Mr. MARKEY. Can I ask one question?

Mr. STEARNS. Oh, absolutely. Okay. Mr. Markey is recognized for 5 minutes.

Mr. MARKEY. Thank you, Mr. Chairman, very much.

Professor Rodotà, Mr. Smith, I note that under the safe harbor the EU has negotiated with the U.S. financial data regulated under the Gramm-Leach-Bliley Act does not qualify for the safe harbor. I believe this was a wise decision on your part, since the privacy provisions of that Act are a pathetic joke.

For example, under the Act, a consumer's consent does not have to be obtained in order to transfer data between separate affiliates. All of these secrets that you have as they all—as they merge—insurance and brokerage and banking, as they all merge, you don't have any privacy.

You can't protect the secrets of your health care, of your family, from being transferred, between separate affiliates in the holding company or with a non-affiliated third party who have entered into a joint marketing agreement with a financial institution.

In addition, consumers have no access and correction rights. Since the charter of fundamental rights of the European Union specifically calls for consent and access and correction rights, will the EU continue to resist including this totally inadequate Gramm-Leach-Bliley Act within the safe harbor?

Mr. RODOTÀ. You know why the financial institutions are not qualified. Because if you look at the memorandum related to the safe harbor enforcement overview, there is a problem because FTC has no jurisdiction for this area. And the U.S. Government has notified only two bodies for the enforcement—FTC and Department of Commerce.

So you can see that there is a problem for this kind of——

Mr. MARKEY. Is it going to continue to be a problem for you?

Mr. RODOTÀ. No. We may have now the possibility to use standard contractual clauses. I think that that—now they have this opportunity.

Mr. MARKEY. So you have an opportunity to lower the privacy standards in Europe?

Mr. RODOTÀ. Too low now.

Mr. MARKEY. No.

Mr. RODOTÀ. No, no.

Mr. MARKEY. You won't lower them.

Mr. RODOTÀ. No, no, no.

Mr. MARKEY. Oh, good. That is what——

Mr. RODOTÀ. That is myself——

Mr. MARKEY. Thank you. I see, yes.

Mr. RODOTÀ. [continuing] negotiating, but the Ambassador I don't know, but I am——

Mr. MARKEY. Okay.

Mr. RODOTÀ. [continuing] on this point.

Mr. MARKEY. Now, Professor Rodotà or Mr. Smith, are you aware that last year the Clinton Administration submitted draft legislation which Representatives the LaFalce and Dingell and I introduced to close these loopholes in the Gramm-Leach-Bliley Act.

Unfortunately, the Republican majority did not take up our bill. We are hopeful that the Bush Administration will take a far more favorable view. Has the EU asked the administration whether it intends to close the loopholes in the Gramm-Leach-Bliley Act, which make it inconsistent with the EU privacy directive?

Mr. SMITH. I mean, I can't really add to the answer I gave, I am sorry. I was asked about this by one of your colleagues before you——

Mr. MARKEY. You can just answer yes or no then. Have you asked them to adopt——

Mr. SMITH. No. As far as I know, and I cannot speak on behalf of the European Commission, there has been no request and there has been no decision in relation to the Gramm-Leach-Bliley legislation. It was put to one side during the safe harbor arrangements and has not been returned to.

And the answer I gave before, I suggested some reasons why there could be difficulties in considering that legislation adequate. And you have—and the question added to that explanation.

Mr. MARKEY. I just wanted you to know, because my time is going to expire, that many people in our country say, "Oh, we are not like the Europeans. They like a lot more privacy than we like here in the United States." But when they poll in the United States, 85 percent of Americans want the same privacy that you give to your citizens.

And I think the reason is is that most of our grandparents came from your countries, and you can't wash your family values out in a generation in the United States. And so the polling is identical, and the only way in which we don't adopt your standards is that the Republicans won't allow us to have a clean vote on the floor of the House of Representatives.

Because if we did, everyone would be forced to vote for it, because 85 percent of the American people want it. So you should just understand that the whole process is aimed toward not allowing any votes on the floor of the Congress, because there would be an overwhelmingly favorable vote to do exactly what you have done because we feel exactly like those from Ireland and Germany and France and Italy, etcetera, etcetera, feel about the very same health and financial services and other information issues.

But there is a large corporate sector here that for some reason or another doesn't want to have a fair vote out on the House floor, and that is why they are sitting out there behind you.

Okay. Just so you understand that.

So keep up the good work. Okay?

Thank you, Mr. Chairman.

Mr. STEARNS. The gentleman has 2 seconds left.

We thank the gentleman for arriving in time, and we appreciate his questions. We assure him that we are going to try to develop a bipartisan bill. With his help, we will be able to do that.

Well, we have just finished, as I said earlier, the first panel, and we have a vote in place. And we understand it is going to be successive votes between 12 and 1. And so we are going to motion to adjourn, and I think until 1. I think that is what I hear from the House, that we are going to have continuing votes here up until 1. So I appreciate that, to panel No. 2, have a nice lunch, and we will see everybody back here at 1.

[Brief recess.]

Mr. STEARNS. The Subcommittee on Commerce, Trade, and Consumer Protection will reconvene, and I thank panel two for waiting. We had a number of votes, and we are going to continue on. We know all of you have planes to catch.

So, panel two, we have Ambassador David Aaron, former Undersecretary of Commerce for International Trade, U.S. Department of Commerce; Mr. Jonathan Winer, former Deputy Assistant Secretary for International Law Enforcement, U.S. State Department; Professor Joel Reidenberg, Professor of Law at Fordham University School of Law; Mr. Denis Henry, Vice President, Regulatory Law, Bell Canada; and Ms. Barbara Lawler, Customer Privacy Manager at Hewlett Packard.

Thank you very much, sincerely, for waiting for us. We are very pleased to have your opening testimony, and we will just start maybe just from the left and go to the right here, my left.

So we would start, then, with Ambassador Aaron.

STATEMENTS OF DAVID L. AARON, SENIOR INTERNATIONAL ADVISOR, DORSEY & WHITNEY LLP; JONATHAN M. WINER, COUNSEL, ALSTON AND BYRD LLP; JOEL R. REIDENBERG, PROFESSOR OF LAW, FORDHAM UNIVERSITY SCHOOL OF LAW; DENIS E. HENRY, VICE PRESIDENT, REGULATORY LAW, BELL CANADA; AND BARBARA LAWLER, CUSTOMER PRIVACY MANAGER, HEWLETT PACKARD

Mr. AARON. Thank you very much, Mr. Chairman. Let me thank you and the committee for inviting me to testify on the European Union's Personal Data Protection Directive and its implications for U.S. privacy law.

It is important to recognize that while we and the Europeans share many basic values, the EU directive comes from a different legal tradition and historical experience, including the police states and the holocaust of the last century. The EU directive attempts to set up a comprehensive personal data protection regime that tries to anticipate every problem and answer every question. It is enforced by a system of independent data privacy commissioners in each of the member states.

While its goals may be laudable, there are a number of fundamental problems with the European directive. First, it was conceived over a dozen years ago when there was no World Wide Web and information technology was dominated by mainframe computers, not distributed information networks, laptops, and digital assistants. As a result, the directive is often rigid or silent in dealing with privacy issues growing out of new technology and new business models. Many European states have had great difficulty translating it into national law.

Second, one can read the European Personal Data Protection Directive from end to end and not find the word "privacy." Although the Commission—the statement on human rights talks about respecting private and family life, the personal data protection is an obligation of the states toward its citizens. In America, we believe that privacy is a right that inheres in the individual.

We can trade our privacy—our private information for some benefit if we choose. In many instances, the Europeans cannot. This can have an important implication when it comes to electronic commerce. But the most troubling aspect of the directive for the United States is the requirement that personal data only be transmitted from Europe to countries that have "adequate" privacy regimes. In effect, the directive would embargo European personal data to any country whose privacy policies, including the United States, the EU had not approved.

Imagine, no transatlantic bank connections, no transatlantic brokerage, no credit card purchases, airline or hotel reservations, no internet or catalog sales, no ability of U.S. firms to manage their operations in Europe, and vice versa. Fortunately, the European Commission recognized that this could hurt Europe as much as it would the United States.

This was the background for the safe harbor negotiations which lasted more than 2 years. Let me briefly describe how the safe harbor emerged and what it is and what it is not.

The first thing we established was that the United States was not going to negotiate a treaty or an executive agreement that

would apply the EU directive in the United States. What we were prepared to do was issue guidance to the American business community on how to conduct commercial relations with Europe.

This comes under the existing authority of the Commerce Department. In the past, we have provided such guidance to help protect U.S. firms doing business in places like the Soviet Union, China, and elsewhere.

The second thing we made clear is that we were not going to accept the jurisdiction of European law in the United States. Indeed, we agreed that the safe harbor would be silent on the issue of jurisdiction. We were prepared to have voluntary self-regulation within the framework of existing U.S. law. We were not going to pass new legislation.

Third, the Europeans had to recognize that we were trying to adapt the directive to the most advanced information economy on earth. Accordingly, the actual provisions of the safe harbor had to be more flexible and address real-world information practices on a reasonable basis. Fortunately, we had the precedent of the privacy principles that we and the Europeans had agreed upon in the OECD many years ago, and this became a touchstone of the discussions.

The European Commission accepted these points but had a bottom line of their own. They insisted on what they considered a high level of privacy protections for European personal data as provided by their directive. It was their information. They had the right to control its dissemination from their point of view.

The result was the safe harbor accord of last year. The Commerce Department promulgated a set of privacy principles for handling European data in the United States. The EU Commission, over the reluctance of many European data protection authorities, and the outright opposition of the European Parliament, held that the safe harbor principles provided adequate privacy protections. Companies that signed up to the safe harbor could receive personal data from Europe without hindrance.

I won't take the committee's time to review the safe harbor principles, but I would like to comment on what aspects of the directive or the safe harbor might be instructive in developing U.S. privacy laws. In doing so, I am drawing on my most recent experience at Dorsey and Whitney where we provide privacy advice to a wide variety of clients as well as my negotiations with the European Union.

First, there is the concept of national privacy standards. The EU developed its directive as part of the effort to create a single market; that is, in order to avoid the complex and burden of having 15 different national privacy laws. I believe that we face a similar risk in the United States, only instead of 15 national laws we could have 50 State laws.

But I have one important caveat. Any Federal privacy legislation preempting State law would have to provide high standards. We need the highest common denominator, not the lowest. If the Federal rule is a minimum standard, for example, that companies merely must have a privacy policy and tell their customers what it is, I think it would be difficult to justify preempting the states.

My second observation draws upon the safe harbor. The essence of that deal was that we accepted high standards and they accepted self-regulation. Any Federal standard should rely, to the extent possible, on self-regulation. That, in my experience, is the best way to avoid high standards from becoming a straitjacket that could smother the information economy.

Thank you very much, Mr. Chairman.

[The prepared statement of David L. Aaron follows:]

PREPARED STATEMENT OF DAVID L. AARON, SENIOR INTERNATIONAL ADVISOR, DORSEY & WHITNEY LLP

Mr. Chairman, let me thank you and the Committee for inviting me to testify on the European Union Personal Data Protection Directive and its implications for US privacy law.

It is important to recognize that while we and the Europeans share many basic values, the EU Directive comes from a different legal tradition and historical experience—including the police states and holocaust of the last century. The EU Directive attempts to set up a comprehensive personal data protection regime that tries to anticipate every problem and answer every question. It is enforced by a system of independent Data Privacy Commissioners in each of the member states.

While its goals may be laudable, there are a number of fundamental problems with the European Directive. First, it was conceived over a dozen years ago when there was no World Wide Web and information technology was dominated by mainframe computers not distributed information networks, laptops, and digital assistants. As a result, the Directive is often rigid or silent in dealing with privacy issues growing out of new technology and business models. Many European States have had great difficulty translating it into domestic law.

Second, one can read the European Personal Data Protection Directive from end to end and not find the word "privacy". Personal data protection is an obligation of the State toward its citizens. In America we believe that privacy is a right that inheres in the individual. We can trade our private information for some benefit. In many instances Europeans cannot. This can have important implications when it comes to e-commerce.

But the most troubling aspect of the Directive for the United States is the requirement that personal data only be transmitted from Europe to countries that have "adequate's privacy regimes. In effect, the Directive would embargo European personal data to any country who's privacy policies the EU had not approved.

Imagine. No transatlantic bank transactions, credit card purchases, airline and hotel reservations, no internet or catalogue sales, no ability of US firms to manage personnel in their European operations, and visa versa. Fortunately, the European Commission recognized that this could hurt Europe as much as the United States.

This was the background for the Safe Harbor negotiations that lasted more than two years. Let me briefly describe how the Safe Harbor Accord emerged and what it is and is not.

The first thing we established was that the United States was not going to negotiate a Treaty or an Executive Agreement that would apply the EU Directive in the U.S. What we were prepared to do was issue guidance to the American business community on how to conduct commercial relations with other countries. This comes under the existing authority of the Department of Commerce. In the past we have provided such guidance to help protect US firms doing business in places like the Soviet Union, China and elsewhere.

The second thing we made clear is that we were not going to accept the jurisdiction of European law in the United States. Indeed we agreed that the Safe Harbor would be silent on jurisdiction. We were prepared to have voluntary, self regulation within the framework of existing US law. We were not going to pass new legislation.

Third, the Europeans had to recognize that were trying to adopt the Directive to the most advanced information economy on earth. Accordingly the actual provisions of the Safe Harbor had to be more flexible and address real world information practices on a reasonable basis. Fortunately, we had the precedent of privacy principles that we and the Europeans had agreed upon in the OECD many years ago. This became a touchstone of the discussions.

The European Commission accepted these points but had a bottom line of their own. They insisted on what they considered a high level of privacy protections for European personal data as provided by their Directive. It was their information; they had the right to control its dissemination.The result was the Safe Harbor ac-

cord of last year. The Commerce Department promulgated a set of privacy principles for handling European Data sent to the U.S. The principles cover notice, choice, transfers to third parties, access, security, data integrity and enforcement. These are accompanied by 15 frequently asked questions that spell out some of the points in detail.

The EU Commission, over the reluctance of many European Data Protection Authorities and the opposition of the European Parliament, held that the Safe Harbor principles provided "adequate's privacy protections. Companies that signed up to the Safe Harbor could receive personal data from Europe without hindrance.

Alternatively, US companies can negotiate contracts with European data suppliers that would follow the Safe Harbor principles but also contain other provisions called for by individual Data Protection Authorities who have to bless the contracts. One US multinational company told me that if they took that route, they would have to negotiate over thousands such contracts.

I won't take the Committee's time to review the Safe Harbor principles, but I would like to comment on what aspects of the Directive or the Safe Harbor might be instructive in developing US privacy laws.

First, the Directive falls short of US privacy expectations in some respects. For example, it provides no special safeguards for protecting children on-line as COPPA does. It also does not protect credit information the same way. As a result, experts have calculated that Europeans pay at least 500 basis point more for consumer credit.

It also goes much further than many Americans might consider reasonable. For example, if a person orders a kosher meal on a flight, the airline cannot store this information for future reference unless the individual explicitly agrees. Why is this considered sensitive information? Because it might reveal the passengers religion or ethnicity.

With these cautionary examples in mind let me suggest how some aspects of the Directive and Safe Harbor could prove useful to any legislative effort. In doing so, I am also drawing on my most recent experience at Dorsey & Whitney where we provide privacy advice to a wide variety of clients.

First there is the concept of national privacy standards. The EU developed its Directive as part of the effort to create a single market—that is in order to avoid the conflicts and burden of having 15 different national privacy laws. I believe that we face a similar risk in the United States, only instead of 15 national laws we could have 50 state laws. But I have one important caveat: any Federal privacy legislation preempting state law would have to provide high standards. We need the highest common denominator not the lowest. If the Federal rule is a minimum standard—for example that companies merely must have a privacy policy and tell their customer what it is—I think it would be difficult to justify preempting the States.

My second observation draws upon the Safe Harbor. The essence of that deal was that we accepted high standards and they accepted self regulation. Any Federal standard should rely to the extent possible on self-regulation. That, in my experience, is the best way to avoid high standards from becoming a straight-jacket that could smother the information economy.

Is Federal privacy legislation timely? In my experience, the answer is clearly yes.

Trust is a continuing issue in e-commerce. Experts estimated last year that the lack of consumer trust cost e-businesses $16 billion in lost sales. More and more companies are seeing the competitive value of providing good privacy practices for their customers. The States are already riding off in different directions on privacy. If high standards can be adopted at the Federal level this will provide American companies with a predictable framework to conduct their business. Even more important, it can provide the American people with greater confidence that their rights will be protected both on-line and off-line to the benefit not only to our economy but to our democracy.

Thank you Mr. Chairman.

Mr. STEARNS. Mr. Winer?

STATEMENT OF JONATHAN M. WINER

Mr. WINER. Thank you, Mr. Chairman. Thank you for the opportunity to testify here today.

I wish to make 10 points about the EU privacy directive. First, it has extraterritorial impact. With the privacy directive, the EU is regulating cyber space and much offline activity as well. E-com-

merce is, by its nature, global. Thus, national laws regulating it tend also to quickly become global.

Following the EU's lead, other countries are adopting privacy laws, some of which, including Canada's, have substantial potential extraterritorial impact. These new laws are global but inconsistent. As we are finding out in the United States, there are many different ideas about how best to regulate privacy. Internationally, we are now facing a maze of conflicting provisions——

Mr. STEARNS. Mr. Winer, could you bring the microphone just a little closer for yourself?

Mr. WINER. Yes, sir.

Mr. STEARNS. Okay. Good.

Mr. WINER. I didn't want to be too loud. Let us try it again.

Internationally, we are now facing a maze of conflicting provisions that create a complex, perilous, and potentially non-navigable environment for the many firms that process personal data which crosses borders. Many of the new foreign privacy laws differ from existing U.S. law, yet because of the transborder nature of many global information flows these laws may, in practice, regulate substantial amounts of data processing within the United States.

If the U.S. is not vigilant, such laws potentially place at risk U.S. competitiveness, U.S. trade, and fundamental U.S. values, including rights protected under the First Amendment as you heard last week.

Second, the privacy directive terms, to the rest of the world, are tantamount to extortion. The EU is requiring that all other countries adopt the EU's privacy laws or risk having data flows to them cutoff by all of the EU's member states. As it has been said, the EU judges which countries in the world have adequate privacy laws. The EU says you don't. EU member states are required by the privacy directive to shut off data flows to that country.

Transatlantic trade and information includes billions of bytes of data each day, and hundreds of billions of dollars in commercial activity a year. The sanction of cutting off such flows is one that cannot be easily activated without threatening fundamental damage to the global economy. The EU has stated it won't implement sanctions if it can find any other way to enforce the privacy directive.

The EU has agreed to a stand-still in enforcement against U.S. firms through at least July 2001. At some point, however, that stand-still will end, and we could have a serious problem.

Third, the safe harbor, unfortunately, is inadequate. Undersecretary of Commerce Aaron negotiated it to secure recognition by the EU that the U.S. system for protecting privacy was adequate, but he was not able to convince the EU to accept that U.S. Federal laws governing privacy in the financial services sector are adequate.

The EU agreed to accept the U.S. system only to the extent that the Federal Trade Commission—and, for a small number of companies, the Department of Transportation—could sue U.S. companies who violate an agreement to live up to principles based upon the requirements of the directive.

This was a very unfortunate outcome. Unlike the EU's lax enforcement of its privacy directive, the U.S. systematically enforces its privacy laws. The U.S. also has a high level of self-regulation.

U.S. regulators have issued detailed regulations governing privacy in the financial services sector, and they examined financial institutions for compliance with U.S. privacy laws.

According to a recent study sponsored by some 200 consumer groups, the U.S. system already protects online privacy better than the EU system. The EU should deem the whole U.S. system adequate and end the threat of cutting off data flows to the United States.

Fourth, the safe harbor is unpopular. The safe harbor has attracted very few takers so far. Only 26 companies have entered as of this week, one of which is here with us today. The tiny number of companies signing up for safe harbor means the vast preponderance of all U.S. companies remains subject to being treated by the EU as inadequately protecting privacy.

Fifth, as was said this morning, the privacy directive threatens national sovereignty. The EU is insisting that it be treated as the de facto global standard for privacy. After July 1st, or whenever the enforcement stand-still ends, all EU member states are supposed to shut down data flows to any company located in any jurisdiction deemed to have inadequate privacy protection.

That is true unless the company subjects itself to EU jurisdiction, EU rules, EU regulations, EU standards, EU courts, and liability to every individual whose information passes to the non-EU company from the territory, physical or electronic, of the EU.

In early 1996, following the shoot-down of an unarmed civilian planes and the murder of U.S. citizens by Cuban MiGs, Congress passed and the President signed the Litertad Act, known by the name of its primary sponsors as Helms-Burton. The Act sought to protect the property rights of thousands of American citizens whose property was confiscated without compensation by the Castro regime, by imposing sanctions on those who profited off that stolen property.

After the U.S. enacted Helms-Burton, the EU issued the following statement. "The European Union is opposed to the use of extraterritorial legislation, both on legal and policy grounds. In the last few years there has been a surge of U.S. extraterritorial sanctions legislation. Such laws represent an unwarranted interference by the U.S. with the sovereign rights of the EU to legislate over its own citizens and companies, and are, in the opinion of the EU, contrary to international law."

In a wired world, literally millions of communications containing personal information go back and forth between the U.S. and the EU every day. A standard that insists that these and other cross-border information flows adhere to an EU privacy regime is in the regime that imposes EU law on the entire world.

And last week I participated in a telephone conversation with an EU official who said, specifically, "Yes. The rules we are applying are going to have global application. You bet."

The privacy directive may fairly be termed the EU's Helms-Burton Act. It seeks to protect a class of property rights by demanding extraterritorial enforcement of those asserted property rights——

Mr. STEARNS. Mr. Winer, we just need you to wrap up.

Mr. WINER. Yes, sir.

Mr. STEARNS. Under the 5-minute rule.

Mr. WINER. My company is based all over the world.

Sixth, the privacy directive is burdensome. My testimony goes into that.

Seventh, it is not a good way of protecting privacy. The principles may look good, but in practice many of them are not workable.

Eighth, do as I say not as I do. The EU is not systematically enforcing it. There is massive non-compliance in the EU.

Ninth, like the privacy directive, the model contracts potentially threaten U.S. competitiveness. They would create causes of action for data subjects who would be third-party beneficiaries of those contracts.

And, tenth, we have the power to protect ourselves from this foreign threat to U.S interest and U.S. economic security. There are a number of options the Congress has in front of it that could help protect us, and I urge you to consider them.

I am happy to respond to any of your questions. Thank you, sir.

[The prepared statement of Jonathan M. Winer follows:]

PREPARED STATEMENT OF JONATHAN M. WINER, ALSTON & BIRD LLP

Mr. Chairman and distinguished members of this Committee: My name is Jonathan Winer. I am an attorney practicing law with the firm of Alston & Bird LLP in Washington, D.C. Previously, I served from 1994 through 1999 as Deputy Assistant United States Secretary of State for International Enforcement matters, where my responsibilities included undertaking negotiations and discussions with the European Union, and its executive implementing body, the European Commission, on a range of Trans-Atlantic matters. Prior to that, I served in the Senate for many years as counsel to U.S. Senator John Kerry (D-Mass.), during which time I worked on international, banking, and legal matters before the Foreign Relations, Banking, Commerce, and Judiciary Committees. Currently, I spend much of my time writing, lecturing, and counseling U.S. companies about privacy issues, including the EU Privacy Directive that is the subject of this hearing.

Privacy is a fascinating and rapidly growing area of the law, and the issue is an exceptionally complex one. I commend this Committee for recognizing its importance and for initiating this set of hearings, and am grateful for the opportunity to testify before you.

1. THE EU IS WRITING RULES REGULATING CYBERSPACE.

If there is anything that is growing at an even more exponential rate than e-commerce, it is laws that purport to govern e-commerce, and in particular, laws governing privacy. Since e-commerce is by its very nature global, national laws regulating it tend also to quickly (and sometimes unintentionally) become global, raising from the beginning the question of whose law will wind up writing the rules by which e-commerce and the World Wide Web operate. While some may want cyberspace to remain a lawyer-free zone, an ever-thickening web of laws is already purporting to determine what activities are permitted, and what activities are prohibited on-line. The vast preponderance of these laws are arising in the European Union, and the most important of them to date is the EU's Directive on Data Protection, known as the "Privacy Directive."[1] Significantly, while many of these laws have been stimulated by consumer and business issues highlighted by new technologies, they would often regulate a far broader swath of activity. In the case of the EU privacy directive, the regulated "industry" would extend to everyone who does business by communicating information about people. Under the Directive, gov-

[1] "Data Protection Directive, 95/46/EC." Other EU laws that purport to regulate various aspects of cyberspace and the world-wide net include, but are not limited to, the EU Directive on E-Commerce (2000), which mandates particular labeling requirements, the Brussels Regulation, which governs consumer rights to sue in their own jurisdiction regardless of contractual terms to the contrary, laws on Access to Justice, Comparative and Misleading Advertising, Consumer Credit and Education, Dangerous Imitations, Long Distance Selling, Information Society, Package Travel, Product Liability, Product Safety, Time Sharing, and Unfair Contract Terms. As a senior European Commission official stated to the author recently, "if it moves, we regulate it."

ernment would regulate and determine what is permitted and what is prohibited communications about all personal data, at least in a commercial context.

Since the passage in 1995 of the Privacy Directive, which became effective in 1998, there has been an explosion of new national privacy laws governing the off-line, as well as the on-line uses of personal data. Within the past twelve months alone, we have seen new data protection laws emerge in Argentina, Australia, Canada, Chile, and Paraguay, following earlier privacy laws in Hong Kong, Hungary, New Zealand, and Switzerland, in addition to the 15 member states of the European Union. Each of these laws is well-intentioned, and addresses what for many is becoming the assertion of a fundamental right—the right of private citizens to own their own personal information. Many of these laws have extra-territorial impact, and some, such as the Privacy Directive, are literally global in their application. Of particular interest is Canada's law, which requires all exporters of Canadian personal data to insure that U.S. companies importing the data agree to apply Canada's laws to the data so long as they retain it, thereby exporting Canada's laws to the U.S. in an almost EU-like fashion. Canada's privacy law could have a profound impact on North American data flows, and on NAFTA, but being only in effect for some two months, its impact remains difficult to measure. [2]

Unfortunately, the laws are not just global, but inconsistent. Like the state legislatures in the U.S., each nation that has looked at privacy has come up with its own constructions for how to protect it. Accordingly, national privacy laws differ from one another on matters of definition, scope, terminology, and application, creating a maze of often conflicting provisions and a potential compliance nightmare for not just for e-commerce, but for any company doing business across borders with individual consumers.

For the United States, the new web of privacy requirements creates some very serious potential problems for our economy and our legal system. Many of the new national privacy laws coming into effect outside the U.S. differ from existing U.S. law, and yet will have the impact of regulating substantial amounts of data processing within the United States. Indeed, in some cases, including the Privacy Directive, the results of the foreign laws will in practice be to create new enforceable legal rights that can be litigated within U.S. courts by Americans and non-Americans alike, regardless of whether Congress, the Executive Branch, or the states have decided that this is a good idea.

The result, for the U.S., is the renewed reminder that foreign countries can enact laws with extra-territorial application. If the U.S. is not vigilant, such laws potentially place at risk U.S. competitiveness, U.S. trade, and fundamental U.S. values, including protected rights under the First Amendment. Each of these areas will be put at great risk by the Privacy Directive in the months ahead, as the EU body responsible for securing its enforcement by the 15 EU Member States, the European Commission, works to insure that its provisions are adhered to by every nation in the world.

2. UNDER THE PRIVACY DIRECTIVE, THE EU DECIDES WHETHER EACH COUNTRY IN THE WORLD'S PRIVACY LAWS ARE "ADEQUATE" OR "INADEQUATE."

Under the Privacy Directive, the EU has decided that privacy is such a fundamental human right that it will permit no one to export personal data from the EU under circumstances that differ substantially from the privacy rules the EU has adopted for itself. Jurisdictions deemed by the EU to have "inadequate" protection of personal data are supposed to be cut off from all the EU's personal data. As Trans-Atlantic trade in information amounts to billions of bytes of information a day, and hundreds of billions of dollars of commercial activity a year, the sanction is one that cannot be easily activated without threatening fundamental damage to the global economy. The EU has recognized this, and has stated that it has no intention of shutting down data flows if it can find any other reasonable solution that adequately protects personal data. A fair amount of forbearance has already been shown by the EU in this regard: although its own 15 member states have been required to be in compliance with the Directive since October, 1998, and several have been taken to court for non-compliance by the European Commission, no country has actually been sanctioned for non-compliance with the Directive to date. Regard-

[2] Canada's law has only been in effect since January 1, 2001, and currently only applies to transborder movements of data that is sold in the commercial context, and not mere processing of personal data. The latter is to be fully covered under Canadian law by January 1, 2004. Interestingly, despite the breadth of Canadian law, the EU has yet to find it to be fully "adequate" under the EU Data Protection standard. To date, only the privacy laws of Hungary and Switzerland, which mirror the EU's, and other states in the EU's economic area have been deemed adequate by the EU.

ing the U.S., the European Commission has agreed to an semi-official stand-still on enforcement against U.S. firms through at least July 1, 2001.

3. THE US-EU PRIVACY SAFE HARBOR: A HOPED-FOR ALTERNATIVE TO A PRIVACY TRADE WAR.

Neither the U.S. nor the EU sought a trade war over privacy. During the Clinton Administration, the U.S., led by Under Secretary of Commerce David Aaron, negotiated in good faith with the EU seeking its recognition that the U.S. system for protecting privacy was adequate. Ultimately, the EU agreed to accept the U.S. system as adequate to the extent that the Federal Trade Commission ("FTC") could sue U.S. companies that agreed live up to a series of principles based upon the Privacy Directive's requirements, and then failed to do so. Such companies could sign up to the EU's privacy standards, and thereby receive a "Safe Harbor" from the sanctions imposed by the EU on firms based in jurisdictions deemed by the EU to have inadequate protection.

Notably, however, Ambassador Aaron was not able to convince the EU to accept that U.S. federal laws governing financial services, including the Fair Credit Reporting Act and the Financial Services Modernization Act of 1999 ("Gramm-Leach-Bliley," or "GLB"), adequately protect privacy, despite clear evidence that these laws are being systematically enforced by U.S. regulators, evidence lacking to date in many cases in the enforcement of EU Member States of the Privacy Directive. Because the EU hasn't found these laws adequate, companies regulated by those laws cannot rely on them for protection against sanctions by EU member states, even if they are in complete compliance with U.S. federal privacy laws.

As a result, the Safe Harbor negotiated by Under Secretary Aaron wound up excluding some of the most important sectors of the U.S. economy, including telecommunications as well as financial services and dramatically limiting its immediate utility.

4. SUPPOSE THEY GAVE A SAFE HARBOR, AND NO ONE CAME?

Notably, in the more than four months since U.S. companies have been able to sign up for Safe Harbor only 26 have chosen to do so as of March 5, 2001. A small number of these are major business-to-business companies, such as Dun & Bradstreet and Hewlett Packard, who have comparatively limited needs for processing personal information by comparison to the many companies whose business are centered on business-to-consumer transactions. Others are self-regulatory organizations such as TRUSTe, the Entertainment Software Rating Board, and the UserTrust Network, for which privacy is the line of business, rather than a requirement of business. The tiny number of companies signing up for the Safe Harbor indicates that the vast preponderance of all U.S. companies remain subject to being treated by the EU as having inadequate protection of privacy.

5. THE PRIVACY DIRECTIVE: THE EU'S HELMS-BURTON?

Under the Privacy Directive, the consequences for having inadequate protection of personal data are simple. Once the current standstill on international enforcement is over—currently set to expire July 1, 2001—all EU member states are supposed (eventually) to shut down the flows of data to any company located in such a jurisdiction, unless that company contractually subjects itself to EU jurisdiction, EU rules, EU regulations, EU standards, EU courts, and liability to every individual whose information passes to the non-EU company from the territory, physical or electronic, of the EU.

In an era of globalized information, the threat to shut down data flows is a remarkable one, but it is the heart of the Privacy Directive. The issue is not one of privacy, but of national sovereignty: should any nation, or group of nations, at this stage of the information economy be threatening to halt data flows to any other nation? In the EU, that is in fact the law imposed by the Privacy Directive, to those who do not provide what the EU deems to be "adequate protection" to personal data.

In early 1996, following the shootdown of unarmed civilian planes and the murder of U.S. citizens by Cuban MIGs in broad daylight and without justification, Congress passed and the President signed the Libertad Act, known by the name of its primary sponsors as "Helms-Burton." The Act sought to promote democracy in Cuba and to protect the property rights of thousands of American citizens whose property was confiscated without compensation by the Castro regime, by imposing sanctions on those who profited off that stolen property.

After the U.S. enacted the Helms-Burton Act, the European Union issued the following statement:

> "The European Union is opposed to the use of extraterritorial legislation, both on legal and policy grounds. In the last few years, there has been a surge of US extraterritorial sanctions legislation both at federal and sub-federal level . . . Such laws represent an unwarranted interference by the U.S. with the sovereign rights of the EU to legislate over its own citizens and companies, and are, in the opinion of the EU, contrary to international law."

The EU complained that it was a violation of international law that the Helms-Burton Act empowered individuals to file private lawsuits against EU companies who were acting in compliance with the terms of their domestic laws.

Accordingly, the EU demanded that the US suspend the right of anyone to sue an EU company under Helms-Burton.

The EU also filed suit in the World Trade Organization against the U.S., seeking a ruling that Helms-Burton violated international trade laws. Eventually, the matter was resolved through a remarkable diplomatic effort undertaken by then Under Secretary of State Stuart Eizenstat, which enabled all the parties to back off from turning a disagreement over policy and property rights into a trade battle.

While Helms-Burton only affected issues pertaining to property in Cuba, one country among some 180 UN member states, the Privacy Directive is global in its application to data that flows out of the EU's borders, and governs not merely real estate or business property but all personal data, except that deemed public under the laws of individual countries. As a result, the Privacy Directive has the consequence of turning the processing of information by anyone, anywhere, at least in a business context, into a regulated industry. The EU's contention that the Privacy Directive only affects information that is exported from the EU and is not extraterritorial makes a debating point, but one that is at odds with the plain facts. In a wired world, literally millions of communications containing personal information go back and forth between the U.S. and the EU every day. A standard that insists that all such information flows adhere to an EU privacy regime is a standard that imposes EU law on the entire world.

It is not unfair to characterize the Privacy Directive as the "EU's Helms-Burton Act," except perhaps to the authors of Helms-Burton, who never dreamed of defining property rights so globally and so extraterritorially.

Indeed, last week, I participated in a conversation with a senior official from the European Commission who explicitly acknowledged this fact in connection with the issuance of new "model contracts" to enable foreign companies to come into compliance with the Directive. She said that the new model contracts soon to be issued by the EU as a base-line for the handling of data from the EU to other countries would have "world-wide application."

The Privacy Directive goes beyond anything contemplated by Helms-Burton in providing for extraterritorial impact on U.S. companies, interference with the sovereign rights of the U.S. to legislate over its own citizens and companies, and permitting EU citizens—and indeed, under certain circumstances—U.S. citizens, to sue U.S. companies for actions that would be legal under domestic U.S. law in connection with the processing of personal data by giving the EU's citizens a global property right in all of their personal information.[3]

6. THE OBLIGATIONS IMPOSED BY THE PRIVACY DIRECTIVE AS IT IS NOW BEING INTERPRETED ARE POTENTIALLY VERY BURDENSOME, ESPECIALLY FOR B2C BUSINESSES.

It can be difficult to make sweeping statements about the meaning the Privacy Directive because different EU entities and persons have interpreted the Directive differently at different times. At one point, for example, the European Commission issued a statement reporting that the Directive protected solely the data of European citizens or residents. Later, this was judged to be incorrect, and the EU made it clear that it applied to all personal data that was being processed within the EU. Moreover, the guardians of privacy within the EU, represented by the EU's "Article 29" Committee, have issued an ever accreting set of standards, guidance, and opinions, with the professed intention of systematically strengthening privacy protection.

---

[3] Elsewhere, I have expressed concerns about the risk to the public space caused by turning personal information into a property right. If every fact about every person, beginning with his or her name and address, becomes private data that he or she controls, what space is left for public communication about public matters? This is a very serious political and policy issue which assumes Constitutional dimensions in the United States, given our history of support for free expression about all matters—including other people—as set forth I the First Amendment. See e.g. "Regulating the Free Flow of Information: A Privacy Czar as the Ultimate Big Brother?", Jonathan M. Winer, The John Marshall Journal of Computer & Information Law, December 2000.

The result is that the obligations for companies under the Directive are to some considerable extent a moving target.

The ultimate level and vigor of the enforcement of the Privacy Directive by EU Member States remains uncertain, and a number of matters of detail pertaining to privacy are still under development by the European Commission. Nevertheless, the parameters of the possible obligations of companies based in the U.S. and other countries whose national laws have not been deemed to be adequate by the EU, currently appear to include:

- Agreeing to submit all of their data processing facilities, files and documents to audit by companies in the EU who are sending them data, and by each of the Data Protection Authorities established in the EU.
- Promising ahead of time to cooperate with each of the EU's privacy czars on any inquiry they may make regarding data processing and to abide by any order the privacy czar chooses to give, regardless of whether the U.S. company considers the order proper, lawful, or practical, and regardless of cost.
- Limiting the use of data only to the purposes for which the data has been transferred.
- Storing the data only as needed to carry out the purposes for which the data has been transferred, and then destroying it.
- Promising not to retransfer the data to an entity in a jurisdiction whose laws are not deemed to offer adequate protection unless the data subject has opted in to such transfer in the case of sensitive data, or has been given an opt-out opportunity in all other cases
- Providing the data subject access to all data relating to him or her being processed in the U.S.
- Allowing the data subject the right to correct or delete data that has become inaccurate.
- Allowing the data subject the right to object to the processing of his or her data on compelling grounds based upon his or her particular situation.
- Naming a privacy officer to handle inquiries from the EU.
- Agreeing to allow anyone whose personal data is transferred from the EU to a firm located in the U.S. to sue as a "third party beneficiary" for violation of any of the above provisions under any contract that permits a U.S. company to import their data. This right to sue would appear to include not just European citizens, but any U.S. citizen whose data has been moved through the EU back to the U.S. Since the right to sue would be a contractual one, in theory that right might well be enforceable by U.S. citizens against U.S. companies in U.S. courts.[4]

7. SOME OF THE BROAD PRIVACY PRINCIPLES LOOK GOOD IN THEORY, BUT MAY NOT BE SMART (OR PROTECT PRIVACY) IN PRACTICE.

Whether the obligations in the Privacy Directive are a good or a bad idea, they are not today the law in the U.S. Indeed, the U.S. Congress has to date declined to make them the law of the U.S. Important arguments can be advanced by reasonable people in favor of and against all of the EU obligations, many of which prove as complex to operate in practice as they are simple to articulate in principle.

For example, the right of access, mandated by the Privacy Directive, states in essence that every person should have to review and correct all the data that is held by any company about them. Stated simply, the right sounds unobjectionable. But many, perhaps most companies around the world, especially large ones, do not centralize their data bases on individuals. Rather, bits and pieces of information about individuals may be contained in many locations at a company. For example, in a Congressional office, each staffer of each Congressman may have their own personal contact directories set up, or case files pertaining to handling the needs of constituents. While some Congressional offices might centralize such data, most would not, and might even view such centralization of data as a potential threat to the privacy of the constituents. To implement a right of access, a company would need to be able to assemble all of its personal data about people easily into one place, for the review of the data subject. The process of assembling and centralizing that data carries with it real risks to privacy, especially if such data can be subpoenaed in civil cases or criminal investigations, both of which are permitted under the Directive. The problem becomes especially severe with large companies which have many different consumer divisions that handle personal information. Is it really good privacy

[4] Some of the above provisions can probably be avoided by a U.S. company that enters the Safe Harbor, but only to the extent that the data flows go from the EU to the U.S. and do not also include, for example, another country such as India or Mexico.

policy to require such companies to centralize all of the data they may possess on all data subjects in order to permit them to easily provide consumers a right of access and correction? In the case of an internet service provider, would that include all identifiable references to these persons on the e-mail traffic processed by the company? Certainly, there are fair arguments to suggest that such centralization may in fact threaten, rather than protect, privacy.

These issues become even more complex when they are taken beyond the context of mainframe computers—the technology that was the main concern at the time the Directive was conceived—to intranets, extranets, e-mails, telecopies, the World Wide Web, lap top computers, smart phones, and hand-held wireless communicators, all of which are theoretically fully subject to the Privacy Directive's requirements for consent, notice, access, uses limited to consent, right to correct, and so on.

Other privacy rights guaranteed in the Directive may prove to of equal simplicity in statement, and equal complexity in practice. As former Clinton Administration privacy czar Peter P. Swire and Brookings Professor Robert E. Litan have written about the Directive, in their book "None of Your Business,":

> "Under the European Directive, many routine and desirable transfers of information would apparently be restricted. For instance, as written, the Directive would appear to hinder pharmaceutical research, could post a major obstacle to investment banks' collection of important information about companies, and would call into doubt many mainframe and intranet applications that involve processing data in the United States or other third countries."[5]

8. NON-COMPLIANCE WITH THE DIRECTIVE WITHIN THE EU IS MASSIVE.

Professors Swire and Litan go on to note that EU officials tell the U.S. not worry about the Directive, that the EU will proceed with implementing the Directive sensibly and incrementally, by encouraging good privacy practices and imposing few penalties on individual organizations. The problem with these assurances, as Swire and Litan state explicitly is that:

> "Europe cannot strictly enforce the letter of the Directive and at the same time announce that organizations can routinely ignore it. It violates the rule of law and fundamental fairness to enforce a law strictly against some while allowing others to violate the same law in the same way . . . An often expressed concern of U.S.-based firms is that they might be targeted for enforcement, even when they follow the same privacy practices as their Europe-based competitors. This targeting may fit the perception that American companies are less careful on privacy issues, and the focus may be politically popular in Europe."[6]

This anxiety is not one that is without merit. Some five years after the passage of the Privacy Directive, the European Commission continues to maintain court action against four of its member states, France, Germany, Ireland, and Luxembourg, for their non-compliance with the Directive. Perhaps more to the point, there is substantial practical evidence that non-compliance with the Directive is widespread throughout the European Union.

Lawyers who practice commercial law involving international businesses see this every day. A few months ago, I was asked by an American company to look at the privacy policies and practices of an EU company that it was purchasing, as part of due diligence, in order to assess the potential risks of liability for the U.S. firm in connection with the purchase. The EU company was in a consumer business that caused it to acquire, process, and manipulate sensitive consumer personal data hundreds or thousands of times every day of the kind theoretically protected by the Privacy Directive. The EU company had no on-line privacy policy. It also turned out

---

[5] Swire and Litan, "None of Your Business," Brooking Institution, 1998, p. 153. The complexity of the compliance issued raised by the Privacy Directive is illustrated by Swire and Litan in Appendix B to their book, which consists of a 12 page chart summarizing some of the potential effects and coverage of the Directive. Among the areas Swire and Litan list as affected by the Directive as mainframes, client-server systems, intranets, extranets, e-mail, telecopies, the World Wide Web, laptop computers and personal organizers, human resources records, auditing and accounting functions, business consulting, calling centers and other worldwide customer service, payment systems for financial services, sale of financial services to individuals, investment banking and market analysis, investment banking "hostile takeovers," which Swire and Litan believe become barred by the Directive; investment banking due diligence, investment banking private placements, mandatory securities and accounting disclosures, individual credit histories, corporate credit histories, the press, nonprofit organizations generally, international educational organizations, international conferences, non-European governments, pharmaceutical and medical device research and marketing, business and leisure travel reservation systems, business and leisure travel frequent flyer and other affinity programs, internet service providers, traditional direct marketing, and direct marketing over the Internet. Id. pps. 248-260.

[6] Id at p. 155.

to have no off-line privacy policy. In fact, it had no privacy policy at all, and after due diligence, we found no evidence that the EU company, had ever undertaken steps to comply with the Directive. Ultimately, we advised the U.S. company, which has comprehensive privacy policies in place, to seek indemnifications from the EU company in case the EU privacy regulator decided to sanction it. The EU company was happy to do so: it advised the U.S. company that in this EU country at least, the actual issuance of penalties for non-compliance with the Privacy Directive and with national privacy laws, was almost unknown.

Thus, it is not surprising that EU consumers groups recently found that Internet users' privacy is better protected in the U.S. than in Europe, despite the Directive and all of the EU's tough national privacy laws. As Consumers International, a UK-based federation of 263 consumer organizations, with members in 100 countries, found in a report released January 25, 2001, assessing 750 top world-wide web sites:

- Despite tight EU privacy legislation, researchers did not find that sites based in the EU gave better information or a higher degree of choice to their users than sites based in the US. Indeed, U.S.-based sites tended to set the standard for decent privacy policies.
- Many EU sites are failing to comply with EU rules that state that they must provide the data subject with the opportunity to opt out if their data is to be used for direct marketing purposes.
- The most popular U.S. sites were more likely than the EU ones to give users a choice about being on the company's mailing list or having their name passed on, despite the existence of legislation which obliges EU-based sites to provide users with a choice.[7]

In short, the ongoing efforts by the EU to require other countries to adopt the EU's standards for the protection of privacy is preceding, rather than following, the EU effectively securing enforcement of its laws within the borders of its Internal Market. The EU is demanding that companies based overseas comply with a Directive that is subject to massive non-compliance within the EU itself.

9. THE FURTHER THREAT POSED BY THE EU'S NEW "MODEL CONTRACTS."

There is little reason for the Congress to delay in considering these kinds of options. The current stand-still on enforcement by the EU is currently due to end on July 1, 2001, at which time U.S. firms who have not entered the Safe Harbor, or who like financial institutions are not eligible for the Safe Harbor, are potentially at risk from EU sanctions. The EU has not stood still while the Safe Harbor process has continued, but has developed as an alternative to Safe Harbor the approach of Model Contracts. These amount to contracts of adhesion whereby non-EU data importers must agree to the jurisdiction, choice of law, substantive law, authority, regulation and oversight by EU data exporters and the EU's privacy czars. These model contracts, discussed in greater depth below, have many risky elements for U.S. firms. Among the most troubling are the requirement in these Model Contracts for joint and several liability for U.S. firms with their EU counterparts for any alleged violation of anyone's privacy; the requirement that data subjects be given the right to sue the U.S. firms for any alleged violation of their privacy; and the requirement that U.S. firms pre-emptively capitulate to whatever the EU chooses to order them to do in the event any EU entity judges them to have violated someone's privacy.

The EU is currently planning to adopt these Model Contracts as a recommended minimum floor of data protection to be enforced by each of the EU's privacy czars as early as this July. In the future, these Model Contracts, or provisions similar to them, or based upon them, could become the de facto minimum standard for the processing of all data by the private sector regarding persons that leaves the EU (other than limited categories of public data.) Their potential risks for U.S. competitiveness, and the risks they pose of creating an unfair burden on non-EU entities throughout the world, can hardly be overstated. Just last week, a senior European Commission official acknowledged that most countries' privacy laws would never be found to be "adequate" under the Directive, and that the Model Contracts would therefore have global application.

It is very important to the components of U.S. industry that are outside the Safe Harbor, including financial services, that the Model Contracts not be used as a mechanism to force them into undertaking obligations that vastly exceed the obligations undertaken by companies permitted to enter the Safe Harbor. It is also important that the Model Contract process not be permitted to overtake, and overwhelm,

[7] Privacy@net, An international comparative study of consumer privacy on the internet, January, 2001, published by Consumers International, and available at www.consumers international.org.

the ongoing talks between the US and the EU on obtaining a finding of adequacy for the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, with their detailed regulations, under the Directive. The EU needs to understand that U.S. laws, too, need to be respected, just as the laws of its Member States must be.

10. OPTIONS FOR U.S. POLICY MAKERS AND THE CONGRESS.

In light of the potential impact of the Privacy Directive on U.S. trade, the exercise of First Amendment rights, and U.S. competitiveness, the U.S. Congress should take a careful look at its range of options. These could include the following, which offered as an illustrative, and incomplete list of possibilities:

- Enacting U.S. federal laws that mimic those of the European Union, granting every person whose information is processed in the United States the right to sue anyone who has used that information for any purpose without their consent. This option risk running into substantial First Amendment and other Constitutional limitations, for the reasons expressed in great detail by Professor Volokh in his testimony before this Committee last week. Exercising this option would also turn every processor of information in the private sector into a member of a regulated industry, requiring a dramatic expansion of government control of the U.S. private sector, providing new opportunities for crowding U.S. courts with allegations of privacy torts, by Americans and overseas persons alike.[8]
- Pressing the EU to recognize, as international consumer groups have, that the U.S. system for protecting privacy is in practice at least as effective as that of the EU, and therefore constitutes adequate protection, eliminating the risk of the disruption of data flows.
- Doing as the EU did in response to Helms-Burton, and treating any efforts by the EU to enforce its Privacy Directive against U.S. companies in a fashion that is extraterritorial as an improper restraint of trade suitable for resolution by the World Trade Organization.
- Doing as Canada did in response to Helms-Burton, and imposing a blocking statute that in effect, prohibits firms from complying with the Directive to the extent that it is inconsistent with U.S. law, and allowing U.S. firms to "claw back" damages from any EU counterparts caused by their use of the Privacy Directive to the injury of the U.S. firm.
- Creating a "Safe Harbor" for U.S. firms that adhere to U.S. federal privacy laws, by making compliance with such a laws a "per se" defense to any private cause of action for alleged breach of privacy or related claims in any court based in the U.S.
- Further developing a regime of informed consent, under which companies that provided mechanisms for consumers to exercise informed consent were given a safe harbor against privacy claims in U.S. courts, so long as they lived up to their contractual obligations to data subjects.
- Asking the U.S. Trade Representative to consider recommending to the President the use of appropriate sanctions under Super 301 or other trade authorities to insure adequate protection of U.S. firms through proportionate measures to respond to any injuries to U.S. companies by the EU.

The Congress has some less dramatic additional interim options which could do much both to protect privacy, the First Amendment, and to simultaneously protect American competitiveness and trade. These include:

- Asking the Executive Branch to secure from the EU a detailed assessment of the existing compliance with the Privacy Directive by firms based in the EU, prior to negotiating further obligations for U.S. firms to comply with the Directive.
- Seeking and obtaining assurances from the EU that no action will be taken against U.S.-based firms for alleged violations of the Directive, until the EU can provide evidence that most EU-based firms have come into compliance with the Directive.

---

[8] See also Swire and Litan, id, at p. 122. "A strict interpretation of the Directive could ban a great many practices by the press. The tension between the press and privacy laws is clear enough: an important responsibility of the press is to publicize personally identifiable information. In reporting on politics, business, entertainment, and sports, journalists routinely discuss named individuals. Often the reporting is done without the consent of the subject . . . Under Article 9 of the Directive, member states can make exemptions for the press, but the exemptions must be 'solely for journalistic purposes' and 'only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.' This language seems to emphasize privacy rights and give relatively little scope to protecting free expression. As governed by Article 9, the press will face compliance difficulties when it transfers personal information out of Europe."

- Seeking and obtaining assurances from the EU that no action will be taken against U.S.-based firms for alleged violations of the Directive until the EU can demonstrate that it has effective mechanisms in place to prevent similar alleged violations by other countries around the world that process substantial amounts of personal data from the EU, including Brazil, China, Egypt, India, Indonesia, Israel, Japan, Malaysia, Russia, South Africa, South Korea, Sri Lanka, Taiwan, Thailand, among others.
- Insuring that EU Member States do not in practice force U.S. firms to enter into "Model Contracts" in order to import personal data from the EU that would create contractual rights for data subjects that would enable them to fill U.S. courts with privacy litigation, including class actions.
- Asking the GAO to determine the regulatory capacity of the U.S. to enforce the existing Safe Harbor and/or the broader parameters of the Privacy Directive were it applied to all processing of personal data by U.S. companies, and to estimate the potential cost of developing the regulatory capacity to administer the equivalent of the Directive in the U.S.
- Asking the Department of Commerce and the Office of the Trade Representative to develop a menu of possible options to respond to any cut-offs of data flows from the EU to the United States and to provide a report to Congress specifying these options.
- Asking the Office of the Trade Representative to review whether data protection laws at the national or EU level may violate the free trade rules administered by the World Trade Organization, a recommendation advocated for consideration several years ago by Professors Litan and Swire, and to develop the analytic and factual basis for making such a case in the event that the EU improperly imposed sanctions on U.S.-based firms.
- Asking the Department of Commerce to catalogue the benefits of maintaining the existing data flows, and to assess the damage that might be done were they to be impeded by enforcement action by the EU under the Privacy Directive,

11. FINAL THOUGHTS.

In conclusion, your Committee has taken on an enormous issue in focusing on the impact of the Privacy Directive on the U.S. The Directive is not, unfortunately, a unique provision. Bit by bit, in its effort to harmonize its own laws for its internal market, the EU is developing other Directives that will come to have an increasingly global impact in setting standards for the whole world. Some of these Directives will surely contain sensible and useful elements. Others may reflect mistaken choices in policy. In either case, the U.S. needs to develop mechanisms to provide early warning on the impact of such Directives on the U.S., on U.S. competitiveness, and on U.S. Constitutional and policy values. The U.S. and the EU come from different histories, and in some areas, such as the area of what is appropriate governmental regulation, from different philosophies. The U.S. economy has been the strongest in the world throughout the years of the ongoing information revolution and the development of the world's new economy. It would be a tragedy if the laws and rules of other jurisdictions were permitted to put our economy at risk, and to threaten the free flow of information so necessary to the world's further economic development, however noble the intentions or lofty the goals.

With your permission, I would like to include with this testimony more detailed analyses of the major provisions of the Privacy Directive and the US-EU Safe Harbor, and of the new Model Contracts being proposed by the EU for adoption and application world-wide later this year.

Thank you. I look forward to responding to any questions, and to providing the Committee with any form of assistance you may request.

* * *

ANALYSIS OF THE EU PRIVACY DIRECTIVE AND THE SAFE HARBOR

A. THE EU PRIVACY DIRECTIVE.

The European Union's Privacy Directive became effective on October 25, 1998. The Directive:

- Embraces individual privacy as a fundamental human right;
- Applies to the processing and transfer of personal data concerning EU residents;
- Requires the EU individual's consent for gathering and dissemination of personal information;
- Applies to all entities that gather, store or use personal data concerning EU residents, including those in the U.S. and every other country;

- Covers personal data transfers not only among affiliates, but even *within a single corporate entity* if the data is exported beyond the EU;
- Includes all data, electronic and non-electronic;
- Demands that data must be destroyed when no longer needed for the original purpose;
- Is enforced in each EU Member State by the Data Protection Authority, which operates independently of the government;
- Provides for civil suits with damages; and
- Provides extraterritorial protections that restrict the transfer of covered personal data to only those non-EU countries that provide an "adequate" level of privacy protection.

B. THE SAFE HARBOR AGREEMENT.

The Safe Harbor Privacy Principles, negotiated between the U.S. Department of Commerce and the European Union and agreed to in July 2000, grant U.S. companies who are subject to the jurisdiction of the FTC or the Department of Transportation a presumption of "adequacy" of protecting personal data for purposes of the Directive, thereby allowing data transfers from the EU to continue to that company. U.S. organizations that choose not to qualify for the Safe Harbor will only be able to transfer data from the EU under one of the allowed exceptions or with an alternative safeguard, such as an EC-approved contract with the EU entity transferring the data--an approach permitted in theory but not yet available due to the European Commission's failure thus far to adopt model contract provisions. In the meantime, the negotiations over treatment of financial services companies have not been completed, leaving banks, savings and loans, and credit unions, other than their affiliates under certain conditions, outside the Safe Harbor.

Briefly, the Safe Harbor:

- Consists of the seven principles of notice, choice, onward transfer, security, data integrity, access, and enforcement;
- Is voluntary;
- Applies forever to all EU personal data received during the company's participation, even if the company later leaves the Safe Harbor;
- Has been available since November 1, 2000 to U.S. organizations through two qualifying options: (1) joining a self-regulatory organization; or (2) implementing appropriate self-regulatory privacy policies;
- Offers protection against direct enforcement by EU Data Protection Authorities ("DPAs"), although if an individual DPA working in conjunction with the FTC finds a violation or "substantial likelihood" of a violation, it will be permitted to bring enforcement against a U.S. company; and
- Does not protect U.S. organizations against private rights of action by EU residents, who may initiate privacy actions under their respective national laws.

1. Signing Up for the Safe Harbor Program.

The U.S. Department of Commerce has had the Safe Harbor program in place and available for participation by U.S. companies on November 1, 2000. As of March 5, 2001, 26 U.S. companies had signed up for the Safe Harbor. There is as yet no fixed date by which U.S. organizations must either join the Safe Harbor or risk disruptions in the transfer of information from EU Member States. The current stand-still on enforcement by the EU runs out on July 1, 2001, although EU officials have privately told U.S. officials that they anticipate extending the standstill for a further period as they continue to efforts to secure compliance with the Directive within the EU's Internal Market..

Safe Harbor members remain subject to the substantive requirements of the Directive and open to private rights of action by EU residents.

2. Qualifying for the Safe Harbor.

There are several methods by which organizations may qualify for the Safe Harbor. An organization may self-certify to the Department of Commerce that:

- It has joined a self-regulatory organization that adheres to the Principles;
- It has implemented privacy policies that conform with the privacy principles of the Directive; or
- It is subject to a statutory, regulatory, administrative or other body of law that effectively protects personal privacy consistent with the Directive. (Note: To date, the EU has not accepted that any U.S. law meets this standard, so this option is not currently available to U.S. companies.)

Alternatively, an organization may enter into EU-approved contracts directly with the entities in the EU that transfer data to the U.S. (Note: This option is also not

yet available in practice, as such contracts must follow forms approved by the European Commission, which has not yet issued such forms. However, the Model Contracts are nearing the completion phase, and are due to be recommended by the relevant committee overseeing the Directive, the so-called "Article 31" Committee, in late March, 2001. Further discussion of the Model Contracts is set forth below.)

Organizations that rely on self-regulation and self-certification are subject to FTC enforcement for unfair or deceptive trade practices with respect to any misrepresentations concerning their adherence to the Principles. Companies that choose to self-regulate and self-certify must provide the Department of Commerce a self-certification letter on an annual basis. The Department of Commerce has agreed to establish and maintain a publicly available list of companies adhering to the Principles. An organization that fails to submit an annual self-certification letter will be removed from the list and Safe Harbor benefits will no longer be assured via this mechanism. Safe Harbor benefits begin on the date an organization self-certifies to the Department of Commerce. Once an organization joins the Safe Harbor, it must apply the Principles to covered data for as long as it stores, uses or discloses the data, even if it subsequently leaves the Safe Harbor.

3. Applying the Safe Harbor's Seven Privacy Principles (Building a Privacy Program).

The Principles are comprised of the basic concepts of notice, choice, onward transfer, security, data integrity, access, and enforcement. Any organization qualifying for the Safe Harbor program must develop a privacy policy that complies with these seven basic principles.

a) Notice. The U.S. organization must provide EU individuals with clear and conspicuous notice regarding the purposes for which it collects and uses their personal information; how to contact the organization with inquiries or complaints; the types of third parties to which it discloses the information; and the choices and methods available to the individual for limiting its use and disclosure (the Notice). Personal data and information are defined in the Principles as "data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form."

The organization must supply the Notice when individuals are first asked to provide personal information or as soon thereafter as practicable, but prior to disclosing the information to a third party or using it for any purpose other than that for which it was originally collected. When disclosing information to a third party that is operating as an agent (such as an outsourcer or other third party service provider), the organization is not required to provide Notice.

b) Choice. A qualifying organization must allow individuals to opt out of: (a) disclosing their information to a third party; and (b) using their information for a purpose other than that for which it was originally collected. The Principles do not define the term "organization," leaving unanswered the question of whether an organization may share data with its affiliates without a formal opt-out procedure.

Individuals must affirmatively consent (opt in) to an organization's disclosure of sensitive personal information to a third party or using it for a purpose other than that for which the information was originally collected. Sensitive information includes personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious beliefs, trade union memberships, information specifying the sex life of the individual, and any information submitted by a third party as sensitive information. There are limited exceptions; for instance, opt-in approval is not required when the sensitive information is necessary to carry out the organization's employment obligations.[9]

c) Onward Transfer. Organizations may only disclose personal information to third parties consistent with the principles of notice and choice. With respect to transfers of personal data to a third party acting as an agent, an organization must determine either that the Agent subscribes to the Principles or is subject to the Directive, before transferring the data. If the agent does not meet one of these requirements, the contract between the organization and the agent must obligate the agent to provide at least the same level of privacy protection as required under the Principles. If an organization complies with this requirement, it will not be held responsible for an agent's improper processing of the personal data, unless it knew or should have known that the third party would process the information improperly.

d) Security. Organizations that collect, maintain, use or disclose personal information must take reasonable precautions to protect such personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

---

[9] *See* Draft, Frequently Asked Questions (FAQs) FAQ 1—Sensitive Data (all FAQs are accessible from http://www.ita.doc.gov/td/ecom/menu.html; hereinafter referenced as "FAQ ____").

e) Data Integrity. Organizations may collect only that personal information relevant to the purpose for which it will be used and must take reasonable steps to ensure that such personal data is not only reliable for its intended use, but is also accurate, complete and current. If an organization is serving merely as a conduit for personal data transmitted by third parties (e.g., ISPs, telecommunications carriers, or others that merely transmit, route, switch or cache information) and does not determine the purposes and means of processing such data, it will not be held responsible for any violation of the Principles by the third parties transmitting such data.[10]

f) Access. The right of access is considered fundamental to the Principles, but it is not absolute. Organizations must give individuals access to their personal information and the ability to correct, amend or delete inaccurate information, except where the burden or expense of providing access is disproportionate to the individual's privacy rights at issue or where the rights of persons other than the requesting individual would be violated.[11] Individuals are not obligated to justify any request for access to their own personal data and organizations are permitted to charge a reasonable fee for such access. If an organization decides to deny access, it must be for a specific reason and the organization must provide an explanation of its decision to the requesting individual.[12]

g) Enforcement. Safe Harbor organizations must implement compliance procedures or mechanisms. At a minimum, this must include: (a) readily available and affordable independent recourse mechanisms by which an individual's complaints are investigated and resolved and damages awarded as provided under applicable law or private sector initiatives; (b) follow-up procedures for verifying that the assertions businesses make about their privacy practices are true and have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles and consequence for violators.

An organization may satisfy the dispute resolution requirements set forth in (a) and (c) above by: (1) agreeing to cooperate with DPAs located in the European Union; (2) complying with private sector-developed privacy programs that incorporate the Principles into their rules and that include effective enforcement mechanisms of the type described in the enforcement principle; (3) complying with legal or regulatory supervisory authorities that provide for the handling of individual complaints and dispute resolution; or, (4) any other mechanism devised by the private sector that meets the requirements of the enforcement principle.

An organization may fulfill the verification requirement of (b) of the enforcement principle either through self-assessment or outside compliance reviews. Under the self-assessment approach, an organization must issue an annual written verification statement, signed by a corporate officer or other authorized representative and made available upon request. [13] Under the outside compliance approach, reviews should be conducted at least once a year and should demonstrate that an organization's privacy policy conforms to the Principles, and that the organization is in compliance.[14]

4. How Violations May Be Enforced .

Violations of the Safe Harbor Privacy Principles may be enforced in several ways. An organization that chooses to subject itself to DPA enforcement must agree to: (a) cooperate with the DPAs in the investigation and resolution of complaints brought under the Safe Harbor; (b) comply with any advice given by the DPAs, including remedial or compensatory measures; and (c) provide the DPAs with written confirmation that such action has been taken. Organizations must comply with the advice of the DPAs within 25 days. If the organization has not complied, or proffered a satisfactory explanation for its non-compliance, the DPA will submit the matter to the FTC or other U.S. federal or state body with statutory powers to take enforcement action. Any failure to cooperate with the DPAs or to comply with the Principles will be actionable as a deceptive practice under Section 5 of the FTC Act.[15]

The FTC has agreed to review on a priority basis any complaints of Safe Harbor violations referred by privacy self-regulatory organizations (such as TRUSTe and BBBOnline) or EU member nations. If the FTC finds a violation, it may seek an administrative cease and desist order (with potential civil penalties) or file a com-

---

[10] *See* FAQ 3.
[11] *See* FAQ 8.
[12] *See* FAQ 8 for a detailed explanation of the access principle.
[13] *See* FAQ 7.
[14] *See* FAQ 7.
[15] *See* FAQ 5.

plaint in a federal district court (with potential civil or criminal contempt charges). If an organization persistently fails to comply with the Principles, it will be denied the benefits of the Safe Harbor.

5. Exceptions to the Principles.

The Principles provide for exceptions in certain limited circumstances. These include: (a) where necessary to meet national security, public interest or law enforcement requirements; (b) where statutes, government regulations or case law create conflicting obligations or explicit authorizations, provided an organization can demonstrate that its non-compliance is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) where the effect of the Directive or a Member State's law is to allow exceptions, provided they are applied in comparable contexts.

6. Current Data Transfers Protected for the Time Being.

Pursuant to Article 26 of the Directive, Member States may permit a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection if: (a) the data subject has given his consent unambiguously to the proposed transfer; (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract in the interest of a data subject between the controller and a third party; (d) the transfer is necessary or legally required on important public interest grounds; (e) the transfer is necessary to protect the vital interests of the data subject; or (f) the transfer is made from a register which, according to laws or regulations, is intended to provide information to the public and which is open to public consultation.

7. Effectiveness to Be Evaluated in 2001, 2003.

The Commission will review the initial progress of the Safe Harbor program in mid-2001. This interim evaluation will be conducted by the Department of Commerce and the Commission to determine whether any organizations have joined the Safe Harbor and whether their privacy programs have been successful. If U.S. organizations are either not participating in the Safe Harbor, or are not complying with the Safe Harbor requirements, the Department of Commerce and the Commission will re-evaluate the Safe Harbor and may at that time set a date by which U.S. organizations must comply or risk disruptions in data transfers from Member States. The Commission will then conduct a more formal review of its decision and the effectiveness of the Safe Harbor in 2003.

8. Timing of Safe Harbor Decision.

For most U.S. companies, there have been three natural opportunities to make judgments about whether to enter the Safe Harbor: (1) the initial period after November 1; (2) the spring of 2001, following the formation of a new Administration and the resumption of U.S. and EU negotiations over financial services; and (3) June, 2001, before the current enforcement stand-still is theoretically due to expire. As set forth above, very few U.S. companies took advantage of the initial period, nor does their currently appear to be a rush to sign up. Most companies have been well-advised to defer their decisions until close to the deadline for the end of the stand-still, when it may become easier to assess actual EU enforcement intentions.

9. Safe Harbor Intended to Provide Predictability and Harmonization.

The Department of Commerce has described the Safe Harbor as providing "predictability and continuity for U.S. and EU companies that are sending and receiving personal information from Europe." [16] The principal benefit ascribed to the Safe Harbor is that it makes automatic the approval by all EU Member States of data transfers to participating U.S. companies, giving a presumptive finding of adequacy for any company that has signed up, articulated its commitment to the Principles, and specified its agreement to an enforcement mechanism. In addition, the Directive is designed to be implemented by laws in each of the fifteen countries that are members of the EU. These laws vary significantly. By providing a single set of data protection rules, the Safe Harbor may offer advantages for companies that operate in more than one EU country.

---

[16] The Safe Harbor Privacy Principles, Frequently Asked Questions and other supporting final documents, including further information on the Safe Harbor list and European Commission supporting documents, are available from the DOC at: http://www.ita.doc.gov. Organizations will also be able to sign up for the Safe Harbor list at this Web site.

At the same time, these benefits come at a significant cost. Participation requires U.S. companies to undertake substantive privacy obligations that go far beyond those required under current U.S. law. The Principles require not merely notice and choice for consumers, but a commitment by the Safe Harbor participant not to transfer personal data to any third party unless the Safe Harbor participant is assured that the third party also adheres to the Principles. Participating companies must also provide access for each individual to all of their personal information held by the organization, and the right to correct, amend or delete inaccurate information. In general, U.S. companies that sign on to the Safe Harbor automatically submit themselves to the jurisdiction of the Federal Trade Commission (FTC), which will have the authority to enforce the Safe Harbor by treating failures to comply with posted privacy policies as unfair or deceptive trade or business practices. Companies that do not abide by their Safe Harbor commitments may also be subject to civil actions for damages brought directly by individual European citizens.

10. Key Terms Still Ambiguous.

Applying the Safe Harbor could be especially complex for U.S. companies whose structure includes multiple corporate units handling different kinds of personal information for different purposes. Key terms used in the Principles, such as "organization" and "third party," remain intentionally undefined because of differences between the U.S. and the EU over the meaning of the terms. These ambiguities make it difficult to determine whether a transfer of personal information is within the "organization" and permissible or to a "third party," requiring consumer consent. Differing interpretations of the law by the individual EU Privacy Commissioners raise other uncertainties, as does the mix of enforcement mechanisms in the U.S. and in the EU.

11. Status of U.S. Financial Institutions Remains To Be Negotiated.

Financial institutions, as broadly defined under the Financial Services Modernization Act of 1999 (the "Gramm-Leach-Bliley" bill or "GLB,") face separate issues. The U.S. and the European Commission were unable to reach agreement that GLB adequately protects privacy, in large part because GLB permits the sharing of personally identifiable information among affiliates. As a result, compliance with GLB for financial institutions is not at this time deemed by the EU to constitute compliance with either the Directive or the Safe Harbor. Because the FTC's underlying authority excludes banks, savings and loans and credit unions from FTC jurisdiction, these financial institutions may not participate directly in the Safe Harbor.[17] The Department of Commerce has advised that applications from such institutions for the Safe Harbor will not be accepted, because of the absence of FTC jurisdiction.

The U.S. and the European Commission have agreed in principle to renew talks in an effort to secure an agreement covering financial services, but these negotiations have yet to move forward in a substantive fashion. In the meantime, the EU stand-still for financial services is expected to remain in place until at least July 1, 2001, and from then, until some agreement is reached between the U.S. and the EU on an enforcement mechanism to permit their participation in the Safe Harbor or compliance with the Directive through other means.

12. How Safe Harbor Works.

When a company signs up for the Safe Harbor, it is obligated to apply the Principles to all data transferred after the date it enters the Safe Harbor, except data that is manually processed. That obligation remains regarding that data forever, even if the company later withdraws from the Safe Harbor. To qualify, a company must also specify to which enforcement agency's jurisdiction it is submitting. At this time, only two U.S. agencies have been granted recognition by the EU for this purpose: (1) the Department of Transportation, for airline carriers, computer reservation systems and other entities it regulates; and (2) the FTC for all other U.S. businesses (except as noted above).

13. Qualifying for the Safe Harbor.

The DOC is administering the Safe Harbor and has posted rules for signing up.[18] The rules include:

- Notification to the DOC by a corporate officer by mail or through www.ita.doc.gov/ecom that the organization adheres to the Principles;
- A request to be put on the Safe Harbor List;

[17] See 15 U.S. C. § 45(a)(2) and § 45(a)(f)(1), for a description of the FTC's jurisdictional limits.

[18] See http://www.ita.doc.gov.

- Public declaration by the organization that it adheres to the Principles and the inclusion of this statement in a published privacy policy; and
- Specification that it is subject to the jurisdiction of the FTC or the Department of Transportation, and further specification of any self-regulatory body, such as TRUSTe or BBBOnline, whose rules it is applying as a means to adhere to the Principles.

C. ANALYSIS OF THE NEW EU MODEL CONTRACT FOR PERSONAL DATA TO COMPLY WITH THE EU PRIVACY DIRECTIVE

As part of securing global compliance with its Directive on Data Protection (the Directive), the European Union is nearing adoption of "Model Contracts" to govern the transfer of personal data from the EU to the United States. New draft Model Contracts are currently under review at the European Commission in Brussels, and final action could come as soon as June, 2001. To date, the U.S. government has not taken a position on the Model Contracts, despite their broad potential impact on U.S. companies.

The new Model Contracts obligate U.S. importers of data to comply with substantive EU data privacy law containing requirements far more onerous than those applicable in the United States. Compliance with the legal obligations embodied in the Model Contracts could create very substantial costs for U.S. companies and impact the U.S. and global economies.

Once approved by the EU, the Model Contracts would permit an EU entity to send personal data to a company located in a country, such as the U.S., that the EU has not yet deemed to have "adequate protection" in place for personal data. The Directive indicates that adoption of a Model Contract is one means of achieving adequate protection. Under the terms of the U.S.-EU Safe Harbor agreement on data privacy made in July, 2000, entry by a U.S. company into the Safe Harbor is another means of achieving adequacy of protection. However, the Safe Harbor is not available to certain types of companies such as financial institutions and telecommunications companies, leaving them potentially no alternative to the Model Contracts. Furthermore, recent comments by EU officials may cast doubt upon the Safe Harbor as a fully sufficient means of satisfying EU regulatory requirements. As no other means of providing adequacy of protection has been approved by the EU, Model Contracts may come to be required for many U.S. companies receiving personal data from the EU.[19] Notably, the EU intends to create an exception to this requirement for a non-EU company that is merely processing data on behalf of an EU company and that exercises no control over the data.

The Model Contracts raise questions of U.S. sovereignty. Under the Model Contracts, *U.S. firms would be required to apply EU substantive privacy law to their operations extraterritorially and to submit to EU jurisdiction and auditing of their facilities. They also would have to accept joint and several liability, as well as the right of all data subjects whose data is exported from the EU to sue for alleged violations.* U.S. parties to the Model Contracts would have to provide all EU data subjects the right to access and correct all of their personal data, and the right to stop its use for any purpose beyond the original consent.

The Model Contracts have come in "under the radar" while attention was focused on the Safe Harbor, negotiated last year between the U.S. and the European Union.[20] The Safe Harbor provides U.S. firms who sign up to it a finding of "adequacy" under the Directive, thus protecting them from possible disruptions in data flows by EU Member States. But to date, only a handful of U.S. firms have signed up to the Safe Harbor. As such, the EU's drive to create the Model Contracts and its apparent move to require them for transactions not covered by the Safe Harbor appears to be an attempt to fill the wide gap left by the narrow impact of the Safe Harbor.

The EU has advised that it intends to move forward with the adoption of the Model Contracts sending them to the European Parliament for consideration, over the course of the spring. The Commission has advised that the Model Contracts could enter into force as early as July 1, 2001, the end of the current standstill for enforcement of the Directive against U.S. firms. In practice, this deadline, like any

[19] It is not yet clear the extent to which existing contracts between EU and US firms governing the processing of personal data from controller to controller will be grandfathered and renewable. The European Commission has informally stated that it anticipates existing contracts will remain lawful, but that the Data Protection Authorities will have the discretion to require tougher privacy obligations as such contracts are renegotiated.

[20] See Alston & Bird LLP Electronic Commerce and International Regulatory Advisory, "The EU Safe Harbor—Should Your Company Sign on Now?," dated October 30, 2000 and located at: http://www.alston.com/docs/Advisories/199709/The__EU__Safe__Harbor.pdf.

political timetable, remains subject to change. Significantly, July 1, 2001 is also the deadline for compliance by U.S. financial institutions with the privacy provisions of the Gramm-Leach-Bliley Act.

U.S. ADMINISTRATION CONSIDERING RESPONSE.

The Bush Administration is currently in the process of considering responses to EU queries regarding the Model Contracts. Newly arrived policymakers at the Departments of Commerce and Treasury are now considering whether to act to slow the EU's adoption of the Model Contracts, given their potential impact on substantial sectors of the U.S. economy and on trans-Atlantic data flows.

If the Model Contracts are adopted, and the U.S. government does not object, U.S. firms who control personal data that comes from the EU, and are not part of the Safe Harbor, will, in essence, be forced to rapidly adopt new information management practices required by EU regulations. Such companies may wish to examine their current information management practices against the emerging laws, regulations, codes, and guidelines in the EU, to determine the feasibility and costs of compliance.

For now, U.S. companies concerned about the potential impact of the Model Contracts may wish to express their views to the key players in the Bush Administration, which, in addition to the Departments of Commerce and Treasury, include the Office of the Trade Representative, the National Economic Council, and the U.S. Department of State.

AN OVERVIEW OF THE MODEL CONTRACTS.

What Are the Model Contracts?

Under the Directive, the EU has the right to develop Model Contracts that can be used as mechanisms to ensure that EU Data Exporters (Data Exporters) have secured adequate assurances from non-EU Data Importers (Data Importers). The Directive does not, however, specify what elements need to be in the Model Contracts. The EU first promulgated possible text of the Model Contracts on September 29, 2000, providing a two-week window for comment. In mid-January, EU representatives advised the U.S. Department of Commerce of the EU's likely adoption of the Model Contracts in February or March. At the same time, the EU group given the responsibility of developing the Model Contracts by the Directive (known as the "Article 29" Committee), suggested that all data flows from the EU to any non-EU entity would have to be governed by either the Model Contracts or more stringent measures that might be enacted by individual EU Member States who choose to provide even higher levels of protection.

Relationship of Model Contracts to Safe Harbor.

In the past, the EU characterized the Model Contracts as a possible alternative to the Safe Harbor for U.S. firms, and the fundamental alternative for U.S. entities such as financial institutions and telecommunications firms that could not participate in the Safe Harbor. This position finds direct support in the language of the EU-US Safe Harbor agreement. Now, however, comments by EU officials in the "Article 29" Committee that has endorsed the contracts, have advised that the Model Contracts should be viewed as a mandatory "floor" of protections for personal data being exported from the EU. As a result, according to the "Article 29" Committee, the provisions of the Model Contract, or other contracts providing equivalent or greater protections, must be agreed to by any non-EU entity from a country that is deemed to have inadequate privacy laws. For the U.S., the provisions of the Model Contracts would therefore presumably apply to all U.S. firms importing personal data from the EU over which they exercise control, other than U.S. firms that have actually entered the Safe Harbor.[21]

Who Would Be Covered by Model Contracts?

If the new EU position is adopted unhindered, sectoral coverage under the Model Contracts would be extremely broad, reaching most Trans-Atlantic flows of personal data. The EU would require the Model Contracts to be used whenever there was

[21] As set forth in footnote 18, one likely near term exception would grandfather existing contracts already approved by EU data protection authorities for the export of data. Whether or not these contracts could be renewed with their existing provisions if they failed to contain such provisions as guaranteeing data subjects the right to sue as third party beneficiaries, and joint and several liability, is not certain. The Article 29 Committee's statements suggest that such provisions will be mandatory. However, to a considerable extent the Member States will remain free to determine how to use the Model Contracts as they apply the domestic laws in conformity with the requirements of the Directive.

a transfer of personal data within an international or multinational group of companies, within a consortium of independent organizations set up to process international transactions, between independent entities where both companies exercise control over the data, between providers of professional services (such as lawyers, accountants, financial advisers, stockbrokers, and surveyors), or for direct marketing, and insolvency and bankruptcy sales.

Required Elements of Model Contracts.

In the current draft of the Model Contracts, contracts entered into between Data Exporters and Data Importers must create an adequate level of protection for personal data transferred to the non-EU country. The contracts must be entered into for the explicit "benefit of Data Subjects," which would create a private cause of action for anyone who deemed themselves injured by an infringement of their data rights. Under the Model Contracts, the data subjects would have the explicit right to enforce the terms of the contracts as third party beneficiaries. In this instance, the data subject would be free to choose dispute resolution in the forum of his or her choice, including mediation, the courts of the exporting Member State, a forum for disputes provided by the DPA in the exporting Member State, or an arbitration body chosen by the data subject. Although the Model Contracts do not explicitly address the issue of the enforcement of contract rights outside the EU, in theory, a U.S. person whose data is exported from the EU to the US in alleged violation of a provision of a Model Contract would also be a third party beneficiary to the contract, with the right to sue under the contract in the courts of their domicile, such as in the U.S.

Obligations of the Data Exporter.

The draft Model Contracts would require all Data Exporters to warrant that: they have met the Directive's obligations in collecting and processing personal data; they have, before any data is transferred, explicitly informed data subjects that their data could be transferred to a third country if the importing entity entered into a contract containing protective clauses provided by law for this purpose; and they will make the protective clauses available upon the request of any data subject.

Obligations of the Data Importer.

Under the proposed Model Contracts, Data Importers will essentially be required to meet the full obligations of EU entities in handling data. *Indeed, in some respects, the Model Contracts go beyond the literal requirements of the Directive itself, and in pursuit of the ostensible goals of the Directive, would impose entirely new obligations on Data Importers.* Among their most significant obligations, the Model Contracts would require Data Importers to:

- Agree to submit all of their data processing facilities, files and documents to audit by the Data Exporter and the DPAs in the EU.
- Cooperate with the DPA in any inquiries regarding data processing and abide by the advice of the DPA if given.
- Process data in accordance with a body of laws approved by the EU as offering adequate protection, which may include, at the Data Exporter's option, the laws of the exporting EU country, a set of newly-promulgated Mandatory Data Protection Principles, or the laws of the country where the Data Importer is based if found by the EU to offer adequate protection (but only if the importer is not already subject to such laws). Any of these alternatives may include more stringent requirements than the Directive itself.
- Use the data only for the purposes for which the data has been transferred.
- Store data only as needed to carry out the purposes for which the data has been transferred.
- Not retransfer the data to an entity in a jurisdiction whose laws are not deemed to offer adequate protection unless the data subject has opted in to such transfer in the case of sensitive data, or has been given an opt-out opportunity in all other cases. Alternatively, the Data Importer may put a Model Contract in place with its intended transferee.
- Allow the data subject access to all data relating to him or her being processed in the U.S.
- Allow the data subject the right to correct or delete data which has become inaccurate.
- Allow the data subject the right to object to the processing of his or her data on compelling grounds based upon his or her particular situation.
- Name a privacy officer to handle inquiries from Data Exporters and the DPAs.

EU Laws Would Govern Liability for U.S. Firms.

The Model Contract process would not permit U.S. Data Importers freedom of contract with Data Exporters with respect to liability issues. Rather, it would automatically require all Data Exporters and Data Importers to agree to be held jointly liable for damages to data subjects resulting from any unlawful processing or act incompatible with the national laws adopted pursuant to the Directive. The parties remain free to provide for mutual indemnification by contract, but the risk of insolvency in the Data Exporter is thus passed on to the U.S. Data Importer, leaving the data subject protected with the U.S. Data Importer's assets for breaches by either party. Although the U.S. Data Importer may be exempt from liability if it can prove that the Data Exporter is solely responsible for the violation, the burden of proof is shifted onto the U.S. Data Importer in such cases.

Non-EU Firm Must Agree To Abide By EU Decisions Over Privacy Violations.

To import personal data from the EU, Data Importers from countries deemed to have inadequate personal data protections, would be required to abide by the data subject's choice for a dispute resolution forum, in the event that the data subject is a party to the dispute. Permissible choices include a mediation forum, the EU court in the Member State where the Data Exporter is established, a body for dispute resolution provided by the DPA in the Member State where the Data Exporter is established, or an arbitration forum in a country which is party to the conventions on enforcement of arbitration awards. Note that the Data Importer must also agree in advance to abide by the decisions of the DPAs in the EU as if it were a party to the proceedings, even if it has not actually participated in them.

COST AND FEASIBILITY OF COMPLIANCE UNCERTAIN.

This summer, the EU plans to review the effectiveness of the Directive in meeting its goals. As it does, the EU will face the reality that compliance with the Directive is spotty. In some EU countries, such as Spain and the United Kingdom, DPAs have begun to initiate enforcement actions and require privacy violators to pay substantial fines. In other EU countries, including France and Germany, the European Commission is still taking legal action to force the Member State to enact required privacy laws.

In the meantime, neither the European Commission nor any EU country has yet to conduct any published study that would provide guidance as to either how costly compliance might be, or whether complete compliance with the Directive is actually possible, either for larger firms with complex corporate structures, or for smaller and medium-sized enterprises that have limited resources for information management. On the other hand, pressed by the threat of information cut-offs, a number of other countries, including Argentina, Australia,[22] Canada,[23] Hong Kong, Hungary, New Zealand, and Switzerland have now passed data protection laws similar to those of the EU. The tension between the growing web of international data protection laws, and the very limited history of the enforcement of these laws, creates an uncertain and potentially difficult business, information management, and legal environment for many companies who process personal data across national borders.

IMPLICATIONS.

The new EU Model Contracts have the potential to go well beyond the Safe Harbor to impact information practices of U.S. firms. The EU's Article 29 Committee has suggested that it intends to encourage the Member State's DPAs to apply the Model Contracts to most international data flows involving countries that it has not deemed to have adequate personal data protections. Although existing contracts governing data protection would likely be grandfathered for the near term, over time, the DPAs would use the Model Contracts, or their functional equivalents, to ensure that EU jurisdiction, choice of law, regulation, and sanctions govern all data that leaves Europe to such places as the U.S. This approach would deprive non-EU entities of independent recourse in disputes, requiring them to submit to and abide by whatever the data subjects or DPAs decide. In short, it would subject the Data Im-

---

[22] *See* Alston & Bird LLP Electronic Commerce and International Regulatory Advisory, "Foreign Privacy Laws Proliferate: New Laws in Argentina and Australia Have Extraterritorial Application," dated December 19, 2000, and located at: http://www.alston.com/docs/Advisories/199709/Foreign__Privacy__Laws.pdf.

[23] *See* Alston & Bird LLP Electronic Commerce and Financial Services Advisory, "New Canadian Privacy Law Now in Effect; Potential Impact on U.S. Firms Obtaining Personal Information from Canada," dated January 23, 2001, and located at http://www.alston.com/docs/Advisories/199709/new__canadian__privacy.pdf.

porter to the full power of the European Union's national authorities and laws, regardless of where the Data Importer is located.

RECOMMENDATIONS.

Any U.S. company that receives customer or employee personal data from the EU should review its existing information management systems, human resources practices, information collection practices, and information dissemination practices against the requirements of the Model Contracts to determine the extent to which existing systems and practices are in compliance. An assessment should be made of compliance costs for meeting the Model Contracts requirements, including the provisions regarding access rights for data subjects. In light of the fact that the EU Model Contracts have yet to be promulgated, potentially affected firms may wish to consider providing their views on the Model Contracts to relevant policymakers in both the EU and the United States.

Mr. STEARNS. Thank you.

Professor Reidenberg?

STATEMENT OF JOEL R. REIDENBERG

Mr. REIDENBERG. Thank you very much, Mr. Chairman, members. I would also like to commend you for holding today's hearing to explore and understand the international dimensions of the global information marketplace.

As background to the hearing today, I have authored—co-authored two books related specifically to the subjects that we are talking about, and over the last decade have served an expert advisor both to the Congress at the Office of Technology Assessment, the Federal Trade Commission, and to the European Commission. I am here today, though, as a scholar on data protection law and policy.

I prepared a written statement that I ask you to include in the record.

Mr. STEARNS. By unanimous consent, all of the written statements will be made part of the record.

Mr. REIDENBERG. Thank you. And would like to highlight in these remarks three areas from that statement.

The first are the implications of the EU directive here in the United States. From the business perspective, the directive I think has both positive and negative trade effects. On the positive side, which we have not really heard about in today's hearing, the directive harmonizes in the EU marketplace for the 15 member states privacy standards, and establishes their single market for flows of information.

I think that is something that is very important. That is a benefit for American businesses. It means that they operate with one more or less uniform set of standards as opposed to 15 radically different country laws.

On the negative side, the directive will force intense scrutiny and limits on international data flows. This—I would disagree with the assessments that this is an extraterritorial application of European law, because I think that it is the European Union saying, "If it is European origin data, we want to be sure that our local privacy rules are not circumvented overseas."

For U.S. citizens, the directive I think highlights that American citizens are becoming second-class citizens in the privacy world, the global level. Why? American law has simply not kept up with the technology. The directive is being followed around the world. Coun-

tries prefer the European approach to the United States treatment of personal information.

And the consequence for that is that citizens outside the United States will have better legal protection for their privacy in the global marketplace than those citizens within the United States.

The second point that I would like to highlight in my testimony is that the safe harbor solution to assure international data flows I believe is completely illusory. Safe harbor is not going to be a satisfactory way of rectifying the serious weaknesses in American law.

The legal basis for safe harbor in the United States I think is very questionable. The safe harbor is predicated on Federal Trade Commission enforcement under Section 5 and the availability of legal recourse in the United States.

And if we look at the Federal Trade Commission statutory authority, I do not believe that the Federal Trade Commission has the authority to protect foreign consumers under the unfair and deceptive practices jurisdiction in order to advance U.S. business interests. And, in fact, the Supreme Court has interpreted the FTC's authority rather narrowly, and Congress has yet to specifically authorize the FTC to protect foreign consumers.

The proposed recourse I think is rather meaningless. The memorandum that was submitted to the European Commission and approved as part of the package refers, for instance, to tort rights that are available under American law. Well, they don't exist yet. We do not have cases in the United States where court have enforced tort rights for data privacy cases.

The Seal Organizations that are also touted under the safe harbor—and when we look at the membership lists, I think we find it a who's who of privacy scandal-plagued companies. And I think that is very troubling.

If you look at the scope of safe harbor, it is extremely narrow. Most of e-commerce will be outside the scope of the safe harbor because of the choice of law provisions that one finds in the directive. I think that we are going to see the national supervisory authorities within Europe very reluctant to follow safe harbor, and at the same time, as a result, increase the risk for non-safe harbor companies that their data flows will be suspended.

The third and last area I want to focus on are a couple of recommendations, two in particular. The first is that I think the best approach for the U.S. Congress is to establish clear legal privacy rights in the United States. The United States is very rapidly becoming a rogue country when we look at the information marketplace and a haven for unfair treatment of personal information. I think that is something we have to rectify as a matter of good, domestic public policy.

At the international level, I think that it will be particularly important for us to push toward an international treaty to deal with privacy. Privacy implicates core democratic values and markets, market issues, and I think only a treaty will enable us to resolve many of the conflicts that will go—that we will see in the future. That I believe to be the best way to solve some of the problems we have on the horizon with the European Union.

With that, I would like to conclude, and thank you very much for this opportunity.

[The prepared statement of Joel R. Reidenberg follows:]

PREPARED STATEMENT OF JOEL R. REIDENBERG, PROFESSOR OF LAW AND DIRECTOR OF THE GRADUATE PROGRAM, FORDHAM UNIVERSITY SCHOOL OF LAW

Mr. Chairman and Members of the Committee, I would like to thank you for the invitation to testify and to commend you for convening this hearing on the European Union's Data Privacy Directive. My name is Joel Reidenberg. I am a Professor of Law and the Director of the Graduate Program at Fordham University School of Law. As an academic, I have written and lectured extensively on data privacy issues and have co-authored two books related to today's hearing.[1] I am a former chair of the Association of American Law School's Section on Defamation and Privacy and have also served as an expert advisor on data privacy issues for the European Commission, the U.S. Federal Trade Commission and, during the 103rd and 104th U.S. Congresses, the Office of Technology Assessment. I appear today as a scholar on data privacy law and policy and do not represent the views of any organization with which I have had affiliations.

My testimony will focus on four points: (1) the philosophy and content of the EU Data Protection Directive, (2) the implications of the European Directive for US privacy policy, (3) the false hope of the US-EU safe harbor agreement, and (4) recommendations for Congressional action.[2]

1. THE EU DATA PROTECTION DIRECTIVE

a) Background and Underlying Philosophy of European Data Protection

While there is a consensus among democratic states that information privacy is a critical element of civil society, the United States has, in recent years, left the protection of privacy to markets rather than law. In contrast, Europe treats privacy as a political imperative anchored in fundamental human rights. European democracies approach information privacy from the perspective of social protection. In European democracies, public liberty derives from the community of individuals and law is the fundamental basis to pursue norms of social and citizen protection. This vision of governance generally regards the state as the necessary player to frame the social community in which individuals develop and information practices must serve individual identity. Citizen autonomy, in this view, effectively depends on a backdrop of legal rights. Law, thus, enshrines prophylactic protection through comprehensive rights and responsibilities. Indeed, citizens trust government more than the private sector with personal information.

In this context, European democracies approach data protection as an element of public law. Since the 1970s, European countries have enacted comprehensive data privacy statutes. Under the European approach, cross-sectoral legislation guarantees a broad set of rights to assure the fair treatment of personal information and the protection of citizens. In general, European data protection laws define each citizen's basic legal right to "information self-determination." This European premise of self-determination puts the citizen in control of the collection and use of personal information. The approach imposes responsibilities on data processors in connection with the acquisition, storage, use and disclosure of personal information and, at the same time, accords citizens the right to consent to the processing of their personal information and the right to access stored personal data and have errors corrected. Rather than accord pre-eminence to business interests, the European approach seeks to strike a balance and provide for a high level of protection for citizens.

b) Adoption of the Directive

As data protection laws proliferated across Europe during the 1980s, there were significant divergences among those laws and harmonization became an important goal for Europe.[3] In 1995, following the Maastricht Treaty of European Union, the European Union adopted *Directive 95/46/EC of the European Parliament and of the*

---

[1] Paul Schwartz and Joel R. Reidenberg, Data Privacy Law: A Study of US Data Protection Law and Practice (Michie: 1996); Joel R. Reidenberg and Paul M. Schwartz, Online Services and Data Protection and Privacy: Regulatory Responses (Eur-OP: 1998). These books were prepared with funding from the European Commission for DG XIII and DGXV, respectively.

[2] Parts of this testimony are based on excerpts from three articles that I have published: Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 STANFORD L. REV. 1315 (2000); A Movement toward Obligatory Standards for Fair Information Practices in the United States, in VISIONS FOR PRIVACY IN THE 21st CENTURY, Colin Bennet & Rebecca Grant, eds., (Univ. of Toronto Press: 1999); Restoring Americans' Privacy in Electronic Commerce, 14 BERKELEY TECH. L. J. 771 (1999)

[3] For a discussion of divergences in Member State law related specifically to online services, see Reidenberg & Schwartz, supra note 1.

Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4] [the "European Directive"] to harmonize the existing national laws within the European Union. The European Directive sought to assure that all Member States provided satisfactory privacy protection and to assure the free flow of personal information across Europe through the respect of basic, standardized protections.

Under European Union law, a "directive" creates an obligation on each Member State to enact national legislation implementing standards that conform to those defined in the directive. The European Directive requires that national law protect all information about an identified or identifiable individual whether or not the data is publicly available. The European Directive requires that an individual's consent be obtained prior to processing personal information for purposes other than those contemplated by the original data collection. The European Directive allows Member States to further restrict the processing of defined "sensitive" data such as health information.[5] The European Directive restricts the collection and use of personal information not relevant for the stated purpose of processing. The processing of personal information must be transparent with notice provided to individuals for the treatment of their personal information. Organizations processing personal information must provide the data subjects with access to their personal information and must correct errors. The European Directive further requires that organizations maintain appropriate security for the processing of personal information.

For global information networks and electronic commerce, the comprehensive approach inevitably invokes some tension. Without the statutory authority to restrict transborder data flows, the balance of citizens' rights in Europe could easily be compromised by the circumvention of Europe for processing activities. Consequently, the European Directive includes two provisions to assure that personal information of European origin will be treated with European standards. A choice of law clause in the European Directive assures that the standards of the local state applies to activities within its jurisdiction and a transborder data flow provision prohibits the transfer of personal information to countries that do not have "adequate" privacy protection.[6]

In terms of enforcement, each Member State must maintain an independent, national supervisory authority for oversight and enforcement of these privacy protections.[7] Significantly, the European Directive also mandates that Member State law require any person processing personal information to notify the national supervisory authority and the supervisory authority must keep a public register of data processors.[8]

c) Implementation Issues

The European Directive provided a transition period through October 1998 for Member States to transpose the standards into national law. However, as is not uncommon in the European system, nine Member States failed to comply strictly with the deadline. By January 2000, the European Commission began proceedings before the European Court of Justice against France, Germany, Ireland, Luxembourg, and the Netherlands for their delays in transposition. Although each of these countries had strong, existing data protection statutes, the European Commission argued that not all of the standards contained in the European Directive were satisfactorily addressed in the national laws. At present, proceedings before the European Court of Justice continue against France, Germany, and Luxembourg.

Notwithstanding the transposition delays, the harmonization achieved by the European Directive is significant, but does not remove all divergences and ambiguities in the European national laws..[9] By and large, the European Directive creates a strong baseline of protection across Europe. But, small divergences and ambiguity will inevitably exist where the principles must be interpreted by different supervisory agencies in each of the Member States. These remaining divergences in standards can pose significant obstacles for the complex information processing ar-

---

[4] 1995 O.J. (L281) 31 (Nov. 23, 1995)

[5] For insightful discussions of the flaws in consent as a model of privacy protection, see the series of articles written by Paul Schwartz: Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices, 2000 Wisc. L. Rev. 743; Internet Privacy and the State, 33 Conn. L. Rev. 815 (2000); Privacy and Democracy in Cyberspace, 52 Vanderbilt L. Rev. 1609 (1999)

[6] See European Directive 95/46/EC, at Art. 4 (choice of law) and Art. 25 (export prohibition).

[7] European Directive 95/46/EC, art. 28.

[8] *Id.,* art. 18-19.

[9] For an analysis of these divergences, see Reidenberg & Schwartz, supra note 1; Peter Swire & Robert Litan, None Of Your Business: World Data Flows, Electronic Commerce, And The European Privacy Directive 188-196 (1998)

rangements typical in electronic commerce. For example, the European Directive requires that privacy rights attach to information about any "identifiable person".[10] Yet, the scope of this definition is not the same across the Member States; what some Member States consider "identifiable" others do not.[11] Similarly, the disclosures that must be made to individuals prior to data collection may still vary within Europe.[12] These differences can distort the ability and desirability of performing processing operations in various Member States since potentially conflicting requirements might apply to cross-border processing of personal information.

The effect of this challenge to comprehensive standards is, however, mitigated by consensus building options and extra-legal policy instruments that are available in the European system. The European Directive creates a "working party" of the Member States' national supervisory authorities.[13] The Working Party offers a formal channel for data protection officials to consult each other and to reach consensus on critical interpretive questions.

Compliance with the national laws has also been an issue in Europe. The notice and registration requirements, in particular, appear to have a spotty reception. One study conducted for the European Commission questioned whether data processors were adequately notifying their treatment of personal information to the national supervisory authorities [14] and a recent study by Consumers International found that European web sites were not routinely informing web users of their use of personal information.[15] Nonetheless, the existence of the national laws and the penalties do allow for enforcement actions to be taken in these cases of non-compliance.

2. IMPLICATIONS FOR THE UNITED STATES

The European Directive exerts significant pressure on U.S. information rights, practices and policies. The Directive facilitates a single information market place within Europe through a harmonized set of rules, but also forces scrutiny of US data privacy. In this context, the lack of legal protection for privacy in the United States threatens the flow of personal information from Europe to the United States. At the same time, the EU Directive is having an important influence on privacy protection around the world and leaves Americans with legal protections as second class citizens in the global marketplace.

a) The Harmonized European Market Place

Despite implementation divergences, the overall harmonization effect of the European Directive creates a common set of rules for the information market place in Europe. Companies operating within the European Union have the benefit of common standards across the Member States rather than 15 diverse sets of conflicting national rules. This creates a large, level playing field for the treatment of personal information in Europe. With a high level of legal protection available on a cross-sectoral basis, Europeans do not face the same privacy obstacles for ecommerce that currently threaten the American experience. The culture of legal protection in Europe provides European companies with a competitive privacy advantage doing business in Europe over the many American companies that are unaccustomed to applying fair information practices to personal information.

b) Scrutiny of US Data Privacy and European Export Prohibitions

The European Directive requires the national supervisory authorities in each of the Member States and the European Commission to make comparisons between European data protection principles and foreign standards of fair information practice.[16] The European Directive further requires that foreign standards of fair information practice be "adequate" in order to permit transfers of personal information to the foreign destination.[17]

For the United States, this means that both national supervisory authorities and the European Commission must assess the level of protection offered in the United States to data of European origin. Because the United States lacks directly comparable, comprehensive data protection legislation, the assessment of "adequacy" is

---

[10] European Directive 95/46/EC, at art. 2(a).
[11] *See* Reidenberg & Schwartz, *supra note 1*, at 124-126.
[12] Reidenberg & Schwartz, *supra note 1,* at 133-34.
[13] European Directive 95/46/EC, art. 29.
[14] Douwe Korff (ed.), *Existing case-law on compliance with data protection laws and principles in the Member States of the European Union,* Annex to the Annual Report 1998 of the Working Party Established by Article 29 of Directive 95/46/EC (Eur. Comm: 1998).
[15] Consumers Intenrational, Privacy@Net: An International Comparative Study of Consumer Privacy on the Internet (Jan. 2001).
[16] European Directive 95/46/EC, art. 25
[17] Id.

necessarily complex. The European Commission and national supervisory authorities recognize that the context of information processing must be considered to make any determination of "adequacy."

Under the European Directive, the national data protection supervisory authorities and the European Commission must report to each other the non-European countries that do not provide adequate protection. This bifurcated assessment of foreign standards means that intra-European politics can play a significant role in the evaluation of US data practices. While a European level decision is supposed to apply in each Member State, the national supervisory authorities are independent agencies and will still have a degree of interpretive power over any individual case.

The end result for the United States and for American companies is that US corporate information practices are under scrutiny in Europe and under threat of disruption when fair information processing standards are not applied to protect European data. Some commentators have predicted that any European export prohibition might spark a trade war that Europe could lose before the new World Trade Organization.[18] While, in theory, such a situation is possible, an adverse WTO ruling is unlikely.[19]

c) International Influence of the EU Directive

Even with the difficulties of the European approach, countries elsewhere are looking at the European Directive as the basic model for information privacy, and significant legislative movements toward European-style data protection exist in Canada, South America, and Eastern Europe.[20] This movement can be attributed partly to the pressure from Europe arising from scrutiny of the adequacy of foreign privacy rights, but is also due in part to the conceptual appeal of a comprehensive set of data protection standards. In effect, Europe through the European Directive has displaced the role that the United States held since the famous Warren and Brandeis article [21] in setting the global privacy agenda.

d) Second Class Privacy for US Citizens

With the imposition by the European Directive both of harmonized European legal requirements for the fair treatment of personal information and of limitations on transborder data flows outside of Europe, U.S. companies recognize that they will have to respect European legal mandates. Unless American companies doing business in Europe chose to flout European law, US multinational businesses must provide stringent privacy protections to data of European origin when processing that data in Europe or in the United States.

Concurrently, American law and practice allows those same companies to provide far less protection, if any, to data about American citizens. This is a particularly troubling aspect of US opposition to the European Directive's standards. American companies will either provide Europeans with better protection than they provide to Americans or they will treat Americans in accordance with the higher foreign standards and disadvantages those citizens doing business with local US companies.

In effect, the proliferation of European style data protection measures around the world means increasingly that American citizens will be left with second class privacy in the United States and afforded greater privacy protection against American companies outside US borders.

3. THE FALSE HOPES OF THE US-EU SAFE HARBOR AGREEMENT

In response to the risk that Europe would block data flows to the United States, the Department of Commerce entered into negotiations with the European Commis-

---

[18] See Peter Swire & Robert Litan, None Of Your Business: World Data Flows, Electronic Commerce, And The European Privacy Directive 188-196 (1998)

[19] See e.g. Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in Ratcheting Up of U.S. Privacy Standards, 25 Yale J. Int'l L. 1, 50 (2000).

[20] *See, e.g.,* Council of Europe, Chart of Signatories and Ratifications <http://www.coe.fr/tablconv/108t.htm>(visited March 31, 1999) (listing countries that have ratified the treaty on data privacy); Industry Canada, *Task Force on Electronic Commerce: The International Evolution of Data Protection* (Oct. 1, 1998) (visited on March 31, 1999) <http://ecom.ic.gc.ca/english/fastfacts/43d10.htm> (justifying the Canadian proposal for a comprehensive privacy law by reference to the European initiative); Hong Kong, Personal Data (Privacy) Ordinance, Chap. 486 <http://www.pco.org.hk/ord/section_00.html>(Hong Kong statute following European comprehensive model); HUNGARIAN REPUBLIC, THE FIRST THREE YEARS OF THE PARLIAMENTARY COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION 68-72 (1998)(discussing the influence of the European Directive for Hungarian data protection law); Pablo Palazzi, Data Protection Materials in Latin American Countries (Dec. 2000) (http://www.ulpiano.com/DataProtection-LA-links.htm) (detailing the emergence of data protection legislation in Latin America.)

[21] See Samuel Warren & Louis Brandeis, The Right of Privacy, 4 Harv. L. Rev. 193 (1890)

sion to create a "safe harbor" agreement that would assure Europe of the adequacy of protection for data processed by US businesses. In the absence of statutory protection in the United States, the concept was that the European Commission would endorse a voluntary code of conduct that would meet the "adequacy" standard. American businesses could then publicly commit to adhere to this code for the treatment of European origin data and be assured of uninterrupted data flows from Europe.

The lengthy and troubled negotiations on the code began in 1998 between the Department of Commerce and the European Commission. Toward the end of the negotiations, several of the particularly difficult issues were the existence of a public commitment for companies adhering to the code, the access rights and enforcement in the United States. A final set of documents including an exchange of letters, the Safe Harbor Privacy Principles, Frequently Asked Questions setting out interpretative understandings of the principles, and various annexes and representations made to the European Commission by the Department of Commerce and the Federal Trade Commission (collectively the "Safe Harbor") was released in July 2000 [22] and approved by the European Commission.[23]

While the approval was an important short-term political victory for both the US and the European Commission, the safe harbor agreement is unworkable for both sides and will not alleviate the issues of weak American privacy protection.

a) The Political Dimension

For the European side, the United States posed a major problem. American law did not provide comparable protections to European standards and fair information practices in the United States were rather spotty. Yet, European regulators did not want to cause a disruption in international data flows. The prospect of change in US law seemed remote and the European Commission would have serious political difficulty insisting on an enforcement action against data processing in the United States prior to the full implementation of the European Directive within the European Union. Similarly, an aggressive enforcement strategy by a national supervisory authority while transposition remained incomplete could have hampered the national legislative debates on transposition. The Safe Harbor offered a mechanism to delay facing tough decisions about international privacy and, in the meantime, hopefully advance US privacy protections for European data.

On the US side, the Department of Commerce faced strong pressure from the American business community to block the European Directive. The United States was not prepared to respond to the Directive with new privacy rights and the United States wanted to prevent interruptions in transborder data flows. The Safe Harbor became a mechanism to avoid a showdown judgment on the status of American law and defer action against any American companies.

As such, the acceptance in July 2000 of the Safe Harbor by the European Union was a transitory political success.

b) The Dubious Legality of Safe Harbor

In the United States, however, the Safe Harbor faces a serious jurisdictional obstacle to its enforcement—one of the key European criteria for acceptance. The Department of Commerce issued the Safe Harbor documents "to foster, promote, and develop international commerce." [24] The agreement is predicated on the enforcement powers of the Federal Trade Commission under Section 5 of the Federal Trade Commission Act.[25] Indeed, as part of the negotiations, the Federal Trade Commission represented to the European Commission that it "will give priority to referrals of non-compliance with safe harbor principles from EU member states." [26] Yet, the underlying legal authority of the FTC to enforce the Safe Harbor is questionable.

As originally enacted by the Federal Trade Commission Act in 1914, Section 5 applied only to unfair methods of competition.[27] Jurisdiction over any "unfair or deceptive act or practice" was extended to the FTC by the Wheeler-Lea Act of 1938.[28] The stated Congressional purpose was to enable the FTC to "restrain unfair and decep-

---

[22] Dept. of Commerce, Int'l Trade Adm, Notice: Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45665-45686 (July 24, 2000)

[23] Commission Decision of 26 July 2000, Eur. Comm. Doc. 00/520/EC, O.J. L 215 (25/8/2000)

[24] Letter, dated July 21, 2000, from Robert S. LaRussa, Acting Under Secretary for International Trade Administration, U.S. Department of Commerce to John Mogg, Director, DGXV, European Commission <http://www.export.gov/safeharbor/USLETTERFINAL1.htm>

[25] 15 U.S.C. § 45(a)

[26] Letter, dated July 14, 2000, from Robert Pitofsky, Chairman, Federal Trade Commission to John Mogg, Director, DGXV, European Commission.

[27] 15 U.S.C. 45

[28] Ch. 49, 52 Stat. 111 (Mar. 21, 1938)

tive acts and practices which deceive and defraud the public generally."[29] Indeed, contrary to the purpose of the Safe Harbor that protects US business interests in international trade, the Wheeler-Lea Act amendments sought to protect the general public from unscrupulous business practices. In fact, at the time of the enactment, the FTC's jurisdiction expressly excluded foreign commerce not to mention the protection of foreign consumers as envisioned by Safe Harbor.

While the McGuire Resale Price Maintenance Act of 1952[30] expanded FTC jurisdiction into foreign commerce with respect to monopolistic pricing, the U.S. Supreme Court had specifically held that only Congressional amendments could expand the scope of the FTC's authority under Section 5.[31] In Bunte Bros. v. FTC, the Commission unsuccessfully sought an expansion of its interstate commerce authority in the context of anti-trust enforcement.[32] Congress eventually responded with the Magnuson-Moss Warranty—Federal Trade Commission Improvement Act of 1975[33] that was, according to the Senate Conference Report, designed "to improve [the FTC's] consumer protection activities."[34] The 1975 amendments extended the jurisdiction to acts and practices "in or affecting commerce," but at no time contemplated protecting American business interests or foreign consumers.

Hence, the assertion by the Department of Commerce and the FTC that the Safe Harbor comes within the Section 5 jurisdiction is a radical departure from the stated legislative purposes of the statute and in direct opposition to the Supreme Court's restrictive interpretation of Section 5 authority.

Within Europe, the legality of Safe Harbor is also open to question. Under the European Directive, "adequacy" must be assesed in light of the prevailing "rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."[35] However, the Safe Harbor was not yet in existence at the time of the approval by the European Commission. The European Parliament specifically noted this problem shortly before the approval by the European Commission.[36] Similarly, according to the European Directive, the European Commission only has authority to enter into negotiations to remedy the absence of "adequate" protection after a formal finding that the non-European country fails to provide "adequate" protection.[37] Yet, in the context of the Safe Harbor negotiations, the European Commission never made a formal finding.[38] These would appear to be significant administrative law defects. Although the European Commission maintains that the European Parliament did not say that the Commission acted outside its powers and the Member States voted unanimously in the political committee to accept the Safe Harbor,[39] this administrative process problem remains an open question that only the European Court of Justice can resolve and gives the independent national supervisory authorities grounds to vitiate Safe Harbor through strict interpretations of the European Commission's ruling.

In addition, the European Parliament pointed out:

> "the risk that the exchange of letters between the Commission and the US Department of Commerce on the implementation of the 'safe harbour' principles could be interpreted by the European and/or United States judicial authorities as having the substance of an international agreement adopted in breach of Article 300 of the Treaty establishing the European Community and the requirement to seek Parliament's assent (Judgment of the Court of Justice of 9 August 1994: French Republic v. the Commission—Agreement between the Commission

---

[29] S. 1077: Report of the Senate Committee on Interstate Commerce, S. Rep. No. 221, 75th Cong., 1st Sess. (March 19, 1937).

[30] Ch. 745, 66 Stat. 632 (July 14, 1952)

[31] Bunte Bros. v. F.T.C., 312 U.S. 349 (1941).

[32] Id.

[33] Pub. L. 93-637, 88 Stat. 2193, § 201, 15 U.S.C. § 45 (1970 ed., Supp. IV)

[34] Magnuson-Moss-Warranty-Federal Trade Commission Improvement Act, Pub. L. No. 93-637, Senate Conf. Report No. 93-1408 (Dec. 18, 1974)

[35] European Directive 95/46/EC, art. 25(2)

[36] European Parliament Resolution A5-0177/2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000-2000/2144(COS)) (July 5, 2000)

[37] European Directive 95/46/EC, art. 25(5).

[38] The procedure for a formal finding is established in European Directive 95/46/EC, art. 25(4).

[39] See Eur. Comm. Press Release: Frits Bolkestein tells Parliament Committee he intends to formally approve "safe harbor" arrangement with US on data protection, July 13, 2000 <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/harbor5.htm>

and the United States regarding the application of their competition laws (Case C-327/91))" [40]

b) The Limited Applicability

Notwithstanding the validity in either legal system, the scope of the Safe Harbor is very narrow. First, Safe Harbor by its terms can only apply to activities and U.S. organizations that fall within the regulatory jurisdiction of the FTC and the Department of Transportation. As a result, many companies and sectors will be ineligible for Safe Harbor including particularly the banking, telecommunications and employment sectors that are expressly excluded from the FTC's jurisdiction.[41] Second, the Safe Harbor will not apply to most organizations collecting data directly in Europe. Article 4 of the European Directive provides that if a data controller is located outside of the European Union, but uses equipment within the European Union, the law of the place where the equipment is located will be applicable. This provision establishes a choice of law rule that greatly reduces the availability of the Safe Harbor to international business. This provision of the Directive is especially significant in the context of web based businesses where interactive computing means that a European user will always make use of computing resources at the user's location. The courts of Member States, such as France, have shown in other areas a clear willingness to apply the substantive law of the place where an Internet user is located.[42] Hence, in many cases, particularly in the context of ecommerce, the substantive law of a Member State will apply rather than the Safe Harbor.

c) Increased Risk to Non-Safe Harbor Transfers

By implication, the Safe Harbor raises the risks for data transfers by companies that do not subscribe to the code. The approval by the European Commission of Safe Harbor as an "adequate" basis to transfer personal information to the United States implicitly acknowledges that transfers outside the scope of the Safe Harbor will not be adequately protected. Consequently, non-Safe Harbor transfers must be covered by one of the other exceptions to the transborder data flow rules, such as a transfer pursuant to a contractual arrangement.[43]

Ironically, Safe Harbor simplifies the task for national supervisory authorities to block data flows to the United States. The national agencies will readily be able to identify those US companies that do not subscribe to Safe Harbor and have not presented a data protection contract for approval under the European Directive's Article 26 exceptions. In such cases, the presumption must be that the protection is "inadequate" and the data flow must, under European law, be prohibited.

For the United States, the Safe Harbor approach might, thus, compromise many US businesses in a way that a legislative solution would not.

d) Weakening of European Standards and Illusory Enforcement Mechanisms

For the national supervisory authorities in Europe, the Safe Harbor poses a weakening of European standards.[44] In particular, the permissible derogations from Safe Harbor without a loss of coverage are significant. The Safe Harbor exempts public record information despite its ordinary protection under European law. Similarly, the Safe Harbor exempts any processing pursuant to any "conflicting obligation" or "explicit authorization" in US law whether or not such processing would be permissible under European standards. The access standard set out in the Safe Harbor and FAQs also includes derogations that do not exist in European law.

Most importantly, however, the Safe Harbor weakens European standards for redress of data privacy violations. Under the European Directive, victims must be able to seek legal recourse and have a damage remedy.[45] The Department of Commerce assured the European Commission that Safe Harbor and the US legal system provided remedies for individual European victims of Safe Harbor violations. The European Commission expressly relied on representations made by the Department of Commerce concerning available damages in American law.[46] The memorandum presented by the Department of Commerce to the European Commission, however,

---

[40] European Parliament Resolution A5-0177/2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000-2000/2144(COS)) (July 5, 2000), § E(2).

[41] 15 U.S.C. § 45(a)(2)

[42] See e.g. UEJF c. Yahoo!, TGI de Paris, Ord. en référé du 22 nov. 2000.

[43] European Directive 95/46/EC, art. 26.

[44] See Working Party: Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", Opinion 4/2000, Eur. Comm. Doc. DG MARKT CA07/434/00 WP 32 (16 May 2000)

[45] European Directive 95/46/EC, art. 22-23

[46] Commission Decision of 26 July 2000, Eur. Comm. Doc. 00/520/EC, O.J. L 215 (25/8/2000), Art. 1(b)

made misleading statements of US law.[47] For example, the memorandum provides a lengthy discussion of the privacy torts and indicates that the torts would be available. The memorandum failed to note that the applicability of these tort actions to data processing and information privacy has never been established by US courts and is, at present, purely theoretical. Indeed, the memorandum cites the tort for misappropriation of a name or likeness as a viable damage remedy, yet all three of the state courts that have addressed this tort in the context of data privacy have rejected it.[48] The Safe Harbor is also predicated on dispute resolution through seal organizations such as Truste. Yet, only one seal organization, the Entertainment Software Rating Board, proposes any direct remedy to the victim of a breach of a privacy policy and other organizations' membership lists look like a "Who's Who" of privacy scandal plagued companies.

Lastly, the enforcement provisions of the Safe Harbor rely on the FTC. Even if the FTC has jurisdiction to enforce the Safe Harbor, the assertion that the FTC will give priority to European enforcement actions is hard to believe. First, although the FTC has become active in privacy issues recently, the agency's record enforcing the Fair Credit Reporting Act, one of the country's most important fair information practices statutes, is less than aggressive. Second, were the FTC to devote its limited resources to the protection of Europeans' privacy, Americans should and will be offended that a US government agency charged with protecting American consumers has chosen to commit its energies and US taxpayer money to the protection of European privacy in the United States against US businesses at a higher level than the FTC asserts for the protection of Americans' privacy.

Sadly, though, for many American companies, even these weakened European standards impose substantially greater obligations than US law. In particular, the notice, choice, access and correction requirements are only sporadically found in US law. As a result, pitifully few American companies have subscribed to Safe Harbor; indeed, as of March 7, 2000 fewer than 30 companies have signed up.[49]

The upshot of these sui generis standards, unenthusiastic reception and enforcement weaknesses is a likelihood that the national supervisory agencies will be dissatisfied with the Safe Harbor and that the Member States will face great political pressure to suspend the Safe Harbor once transposition is completed.

4. RECOMMENDATIONS

The United States is rapidly on the path to becoming the world's leading privacy rogue nation. Just a cursory examination of the data scandals over the last year and consumer privacy concerns for ecommerce suggest that our national policy of self-regulation will not work to assure public confidence and trust in the treatment of personal information, cannot work to guarantee citizens their political right to freedom of association and privacy, and will leave American businesses at a competitive disadvantage in the global information market place. At a time when Internet growth rates are greater outside the United States and non-US web content is becoming an absolute majority of available Internet content, United States interests are ill-served by avoiding the creation of clear legal privacy rights.

Congress needs to act to establish a basic set of legal protections for privacy in the United States. Any such regulation must recognize that technologies will be essential to assure privacy protections in the global environment across divergent sets of rules. In fact, technical decisions are not policy neutral. Technical decisions make privacy rules and, more often than not, these rules in the United States are privacy invasive. For technology to provide effective privacy protection, three conditions must be met: (a) technology respecting fair information practices must exist; (b) these technologies must be deployed; and (c) the implementation of these technologies must have a privacy protecting default configuration. Legal rights in the United States should provide an incentive structure that encourages these developments.

In conjunction with the establishment of a legal baseline in the United States, Congress should promote the negotiation of a "General Agreement on Information Privacy" within the World Trade Organization framework.[50] Whether desired or not by various interest groups and countries, the WTO will be unable to avoid con-

---

[47] U.S. Dept. of Commerce, Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law (July 14, 2000)

[48] See Shibley v. Time 45 Ohio App. 2d 69 (1975); Dwyer v. American Express 273 Ill. App. 3d 742 (1995); Avrahami v. U.S. News & World Report, 1996 Va. Cir. LEXIS 518 (1996).

[49] U.S. Dept. of Commerce, Safe Harbor List, http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (reflecting only 27 certifications)

[50] See Joel R. Reidenberg, Resolving Conflicting International Privacy Rules in Cyberspace, 52 Stanford L. Rev. 1315, 1359-1362 (2000)

fronting international privacy issues as a result of the biennial ministerial conferences and the inevitable trade-in-services agenda. Many of the core differences among nations on the implementation of privacy principles touch upon fundamental governance and sovereignty questions. These types of problems will only be resolved at an international treaty level like the WTO.

Mr. STEARNS. Thank you.

Ms. Lawler, your opening statement, please? Thank you.

STATEMENT OF BARBARA LAWLER

Ms. LAWLER. Yes. Thank you, and thank you for having me here today. Mr. Chairman, members of the subcommittee, thank you for the invitation to appear today to discuss the EU Data Protection Directive.

My name is Barbara Lawler, and as Customer Privacy Manager for Hewlett Packard I have global responsibility for HP privacy policy management, implementation, compliance, education, and communication, in both the online and offline worlds.

As you, Mr. Chairman, stated in calling for this hearing, the European privacy directive has implications for how we in the United States conduct and address our domestic privacy issues. I am pleased, therefore, to have this opportunity to talk about HP's participation in the safe harbor agreement, which provides legal protection and a framework for allowing the safe transfer of personal information from the EU countries to the U.S.

I am pleased to say that HP is the first major technology company to join the safe harbor. But, first, let me start by giving you an overall picture of how we manage privacy at Hewlett Packard.

HP applies a universal, global privacy policy built on the fair information practices. Notice, choice, accuracy and access, security and oversight. Whether in English, French, or Spanish, the core commitments are the same with very minimal localization required to reflect local country laws.

Key elements of our policy include no selling of customer data, no sharing of data outside HP without permission, customer access to core contact data, and a customer feedback mechanism. The policy can be viewed in online form in the lower left-hand corner of every HP.com web page.

The guiding principles that we operate under for managing privacy are customers control their personal information. We give choices that enhance trust, and, therefore, enhance our business. We put the customer in the lead to determine their relationship with HP and to have the highest integrity and practices, responses, and partners.

A sample of some of our current global efforts in privacy management include moving to opt-in for marketing content, especially e-mail, company-wide training on new privacy standards, new application development and business rules for company-wide multiple customer data base consolidation, and platform for privacy preferences implementation for our most active websites.

I want to underscore some important distinctions around the opt-in discussion and hopefully add some clarity. As I mentioned, it is HP policy never to sell or lease our customer data. We have many business relationships with other companies, companies that act as suppliers and service providers. Those companies are required

under contract and through non-disclosure agreements to abide by our privacy policy.

A different class of business relationships are our strategic partners and co-marketing partnerships. As stated earlier, it has always been HP policy that there is no sharing of customer data outside HP without permission from the customer. This is an opt-in policy for data-sharing with third parties.

Applying the opt-in standard for marketing contact with HP is another order of magnitude more difficult, and let me tell you why. We are committed, because this is absolutely the right thing to do for our customers. What it requires us to do is to evaluate all customer data bases, our customer privacy data choice elements, the data itself, reengineer those data structures, the systems, and all of the associated business processes, change the format of the privacy question we ask our customers, and then develop implementation guides and tools and communicate that new standard HP-wide.

Some of the challenges we are facing is managing conflicting customer choices and a large volume of unknown privacy data choice.

We do conduct a substantial amount of cross-border commercial and consumer business activity between the U.S. and EU, which require direct communications between EU country-based HP offices, independent suppliers and customers, and involves the movement of personal information on a regular basis.

In order to have HP's European offices come into compliance with the EU privacy directive, a multi-country assessment of data collection use, storage, and movement was conducted out of which we identified compliance matches and gaps. Some of our current HP specific efforts in Europe include consolidating our customer e-mail response process and customizing privacy implementation guides for marketing by country.

On January 29 of this year, HP became the first high-tech company to certify under the safe harbor. This demonstrates our continued leadership to strong privacy practices in the U.S., and we believe it is important because it offers consistency and continuity for business operations connected between HP sites located in the U.S. and the EU—critical for a global enterprise.

We believe that consumer confidence will be enhanced by ensuring privacy rights on and offline in a global commerce environment through the safe harbor. E-commerce will grow faster if consumer confidence is reinformed by company efforts to ensure consumers have an effective recourse for privacy complaints through agreements like safe harbor.

Our privacy policy has always been consistent with the safe harbor principles, and we found it consistent with our long-term membership with the BBB Online Privacy Seal Program. We view safe harbor compliance as really the ultimate self-regulatory approach and the next logical commitment in our step to privacy.

And, finally, let me put this into perspective with the larger transborder privacy issue and consumer confidence in the global marketplace, because we know consumers not only are concerned about their privacy but they are also concerned about whether their credit cards are safe online, and if they order a blue vase from a website in Paris that they will get what they ordered.

HP is working with 70 businesses from around the world through the global business dialog for electronic commerce to develop worldwide consensus on standards for consumer redress systems and ADR. Current concerns about consumer confidence must not be allowed to turn into barriers for empowering consumers——

Mr. STEARNS. Ms. Lawler, we need you just to sum up, if you would.

Ms. LAWLER. I am. HP believes that the safe harbor agreement is a significant step in the right direction, and we welcome the opportunity to work with this subcommittee in the development of national policies governing the collection and use of personal information.

[The prepared statement of Barbara Lawler follows:]

PREPARED STATEMENT OF BARBARA LAWLER, MANAGER, CUSTOMER PRIVACY, HEWLETT-PACKARD COMPANY

Mr. Chairman, Members of the Subcommittee thank you for the invitation to appear today to discuss the EU Data Protection Directive.

My name is Barbara Lawler, and as HP Customer Privacy Manager, I have global responsibility for Hewlett Packard privacy policy management, implementation, compliance, education and communication, in both the online and offline worlds.

By way of background, HP is a leading provider of computing and imaging solutions and services. As a company we are focused on making technology and its benefits accessible to individuals and businesses through networked appliances, beneficial e-services and an "always on" Internet infrastructure. HP has 88,500 employees worldwide and a total revenue of $48.8 billion in its 2000 fiscal year.

As you Mr. Chairman, stated in calling this hearing, the European Privacy Directive has implications for how we in the United States will address our domestic privacy issues. I am pleased therefore, to have this opportunity to discuss Hewlett-Packard's participation in the "safe harbor" agreement . The safe harbor provides legal protection and a framework allowing for the safe transfer of personal information from European Union countries to the United States. I am pleased to say that HP is the first major technology company to join the safe harbor.

As a high-tech company that sells to the consumer market, we take the privacy issue very seriously. HP believes that self-regulation and credible third-party enforcement "such as the Better Business Bureau privacy seal program—is the single most important step that businesses can take to ensure that consumers" privacy will be respected and protected online. We also believe that there should be a "floor" of uniform consumer protections which all companies must adhere to; based upon clear and conspicuous disclosure of privacy policies. HP testified last Congress in favor of the McCain/Kerry privacy bill (S. 2928) which we think meets the test of reasonable, practicable privacy protections. And, as I will discuss further, with our own websites, we are moving as quickly as we can, wherever possible, to an "opt-in" environment.

Managing Privacy at Hewlett Packard

Let me start by giving you an overall picture of how we manage privacy at Hewlett Packard. HP applies a universal, global privacy policy built on the fair information practices: notice, choice, accuracy & access, security and oversight. Whether in English, French or Spanish, the core commitments are the same, with minimal localization required to reflect local country laws. Key elements of the policy include no selling of customer data, no sharing of customer data outside HP without permission, customer access to core contact data and a customer feedback mechanism.

The policy can be viewed in online form at the lower left-hand corner of every hp.com web page: http://www.welcome.hp.com/country/us/eng/privacy.htm

The guiding principles for managing privacy in HP are:

- customers control their own personal data
- give choices that enhance trust and therefore enhance the business
- put the customer in the lead to determine their relationship with HP
- have the highest integrity in practices, responses and partners

HP people apply the privacy policy to marketing, support, e-services and product generation using a set of HP-developed tools called the "Privacy Rulebook" and the "Web Site Data and Privacy Practices Self-Assessment Tool".

A sample of current HP global privacy initiatives include:

- moving to opt-in for marketing contact, especially e-mail
- company-wide training on new privacy standards
- new application development and business rules for company-wide multiple customer database consolidation
- Platform for Privacy Preferences (P3P) implementation for our most active web sites

I want to underscore some important distinctions around the "opt-in" discussion and add some clarity. It's HP policy to never sell or lease our customer data. HP has many business relationships with other companies. Companies that act as service providers or suppliers are required under contract and through a Confidential Non-Disclosure Agreement to abide by HP's privacy policy.

A different class of business relationships is HP's strategic partnerships and co-marketing partners. As stated earlier, it's always been HP policy that there is no sharing of customer data outside HP without permission from the customer. This is an opt-in policy for data sharing with third parties.

Applying the opt-in standard for marketing contact within HP is an order of magnitude more difficult, but we're committed because it's the right thing to do for our customers. Implementing opt-in for marketing contact requires us to evaluate all customer databases and customer privacy choice data elements, re-engineer the data structures, systems and associated processes, change the privacy question format itself, develop implementation guides and tools, and communicate the new standard hp-wide. Some of the challenges we face are in the areas of managing a program-specific customer privacy choice with a "top-down" HP request and resolving a large volume of "unknown" privacy choice data.

Managing the EU directive in an intra-European environment

In addition to the core universal HP privacy practices already described, HP has developed specific standards, practices and tools to operate within the framework of the European Data Protection Directive in our European country organizations. These were developed out of a cross-functional HP task force with representatives from Customer Information, Human Resources, Privacy Management, Legal, Risk Management, Information Technology and Workers Council delegates.

HP conducts a substantial amount of cross-border commercial and consumer business activity between the US and EU countries. This requires direct communications with EU country-based HP offices, independent suppliers and customers, and involves the receipt and sharing of personal information from them on a regular basis. In order to have HP's European offices to come into compliance with the EU privacy directive, a multi-country assessment of data collection, use, storage, and movement was conducted, out of which were identified compliance matches and gaps. Industry benchmarking was conducted concurrently. From there specific action plans were developed and the following deliverables completed:

- IT/Application Data Privacy Sensitivity and Development Checklist
- Confidential Non-disclosure agreement for contracts with suppliers
- Personal Data(base) Access Standards for employees
- Data Protection Clause—Individual Undertaking Agreement for employees
- Data Protection Officer for HP Germany
- Data Protection Officer—HP European Region (in process)
- Customer Privacy Manager—HP European Region (in process)
- Establishment of European Region Privacy Council (pending)

Current HP European-specific efforts include consolidating the customer email response process for privacy questions and customized privacy implementation guides for marketing programs by country.

Managing the EU directive requirements in the US (Safe Harbor)

On January 29th, 2001, HP became the first high-tech company to certify with the U.S. Department of Commerce for Safe Harbor. This demonstrates our continued leadership to strong privacy practices in the U.S. The Safe Harbor framework offers consistency and continuity for business operations conducted between HP sites located in the United States and the European Union, critical for a global enterprise. HP has certified data collected by online, offline and manually processed methods. HP conducts a substantial amount of cross-border commercial and consumer business activity with direct involvement of EU country-based HP offices and independent suppliers.

We believe that consumer confidence will be enhanced by ensuring customer privacy rights on- and off-line in a global commerce environment. E-commerce will grow faster if consumer confidence is reinforced by company efforts to ensure consumers have an effective recourse for privacy complaints through agreements like the Safe Harbor.

The practices described in the HP privacy policy have long been consistent with the Safe Harbor principles. As a member of the Safe Harbor compliant BBBOnLine Privacy Seal program for the last 16 months, we were pleased to see close alignment between our existing privacy policy and the Safe Harbor Principles. The verification requirements mapped well to existing internal HP privacy standards and practices.

HP views Safe Harbor compliance as a self-regulatory bridge to different approaches to data privacy between the United States and European Union; it's the ultimate "self-regulatory" approach. Joining the Safe Harbor is the next logical step in our commitment to privacy protection.

Finally, I would like to put the trans-border privacy issue into the larger perspective of consumer confidence in the global electronic marketplace. While consumers are concerned about their privacy online, they are also concerned about whether their credit cards are safe online, and whether if they order a blue vase from a website in Paris or Tokyo, they will get what they order in the quality and condition they expected. In order for online businesses to truly earn the trust of consumers, we need to expand ongoing efforts to ensure that the global electronic marketplace a clean, well-lighted venue for both consumers and businesses. For example, consumers need to have confidence that when they do business across national borders, that there will be a redress system in place should anything go wrong with the transaction.

HP is working with 70+ businesses from around the world through the Global Business Dialogue for electronic commerce to develop worldwide consensus standards on consumer redress systems, of ADR. In this effort, we are working with consumer groups and the FTC and the European Commission to ensure that consumers and businesses will quickly, fairly and efficiently resolve complaints related to online transactions.

Current concerns about consumer confidence must not be allowed to turn into barriers to empowering consumers through global e-commerce. Hewlett-Packard believes that the safe harbor agreement is a significant step in the right direction, and we welcome the opportunity to work with this subcommittee in the development of national policies governing the collection and use of personal information.

Mr. STEARNS. Thank you.

Mr. Henry, your opening statement?

STATEMENT OF DENIS E. HENRY

Mr. HENRY. Thank you, Mr. Chairman, for this invitation.

As you mentioned, I am with Bell Canada, so let me begin by telling you who we are. Bell Canada and its affiliates have a wide variety of consumer-facing business activities, and as a result we have been keenly interested in the privacy issue for many years.

We are the largest telecommunications carrier and internet service provider in Canada, and in keeping with the convergence trend we also have a number of investments on the content side of the business, including an internet portal, broadcast television, direct-to-home satellite——

Mr. STEARNS. Mr. Henry, we would ask you just to move your microphone just a shade up there.

Mr. HENRY. Certainly.

Mr. STEARNS. That is good.

Mr. HENRY. Direct-to-home satellite, and, most recently, a national newspaper we have added to the portfolio.

Now, let me turn now to Canada's approach to privacy and our response to it. With the advent of new technologies, a number of options to address the concern about protecting personal information have been debated in various circles around the world. And I would characterize the Canadian approach as lying somewhere in the middle of the spectrum of options.

It is not a detailed and prescriptive regulatory regime. On the other hand, it is not an approach that relies primarily on market forces.

Back in 1996, in response to rising concerns about privacy, the Canadian Standards Association released its model code for the protection of personal information, which we call the CSA Code, as a voluntary national standard. The CSA Code was based on the OECD privacy guidelines and was the product of a consensus-building process involving government, consumers, and key industry sectors.

However, following development of the CSA Code, consumer concerns about privacy persisted. Faced with this environment, the government of Canada undertook broad public consultations to explore the possibility of a legislative approach. These discussions revealed broad support for a self-regulatory approach but assisted by framework legislation that would encourage industry groups to develop sectoral codes based on the CSA Code.

And this ultimately led the Canadian government to enact Federal privacy legislation last year, which is to come into effect or came into effect January 1st of this year. Its objective has been to establish harmonized national rules across the country based on a light-handed and flexible legislative framework.

The Act is also intended to meet the adequate data protection requirements of the EU Data Protection Directive.

This new piece of Federal privacy legislation requires all organizations that collect, use, or disclose personal information to comply with the CSA Code which is appended to the Act, and the Act reflects a flexible approach that does not prescribe particular treatment of personal information, but, rather, organizations can develop codes and practices tailored to their particular business circumstances.

The legislation also requires commercial organizations to identify the purposes for which personal information will be collected, used, and disclosed, and to obtain consent of individuals. Consent can be either express or implied, depending on the circumstances and depending on the sensitivity of the information, and, again, reflecting a flexible approach.

The Act also establishes a Federal privacy commissioner as its prime overseer. This commissioner has broad powers to receive and investigate complaints and to conduct audits of company practices. Unresolved disputes can be taken before the Federal court of Canada for a hearing and enforcement, including the possibility of damages.

Recently, the Bell companies released the Bell Code of Fair Information Practices, in compliance with the CSA Code and the new legislation. And in order to implement this code, the companies have embarked on a plan that incorporates a number of elements.

First of all, procedures were put in place to ensure that customers and employees are able to review and correct company records that contain their personal information. Customer are also able to challenge the company's compliance with the code through the Bell privacy ombudsman.

Second, companies have implemented a communications plan to inform customers of the privacy policies using, for example, a number of means, telephone directories, web pages, bill inserts, point of sale brochures, and so on. The companies are also undertaking

an extensive training program to ensure that employees understand and uphold our privacy commitments.

The companies have also undertaken a comprehensive review of their information systems to ensure that the provisions of the code will be respected. And, finally, regular internal audits will be employed to ensure ongoing compliance.

The Bell companies and many other industry sectors in Canada have supported the Canadian government's steps in pursuing a new model for the protection of personal information, a model that builds on the voluntary efforts of consumer groups, industry, and governments.

We recognize that protecting customers' privacy makes good business sense. But at the same time, this objective must be balanced against the legitimate need to use customer information for business purposes and to avoid overly costly and burdensome regulation.

By enacting a flexible legislative framework, the Canadian privacy approach has attempted to strike an appropriate balance.

I hope these comments, Mr. Chairman, have shed some light on our unique approach to privacy, and I would be happy to answer any questions.

[The prepared statement of Denis E. Henry follows:]

PREPARED STATEMENT OF DENIS E. HENRY, VICE PRESIDENT, REGULATORY LAW, BELL CANADA.

INTRODUCTION:

Thank you, Mr. Chairman, for the invitation to appear before you and the members of the Sub-committee today on this very important subject.

My name is Denis Henry and I am the Vice President of Regulatory Law with Bell Canada, the largest telecommunications carrier in Canada.

As a group, the Bell Companies in Canada provide a full range of communications services to more than eight million residence and business customers. We are among the world's leading communications organizations, with core investments in telephone networks, both wired and wireless; Internet Protocol (IP)-based networks and solutions; electronic commerce; systems integration; directories and satellite networks. We are a major player in the local exchange, long distance and Internet access markets, including high speed access. On the content side of the business, we have investments in cable programming channels, broadcast television, a multi channel video program distributor through our direct-to-home satellite service, an Internet portal, new media and most recently a national newspaper. Given all of these varied business activities, most of which deal directly at the consumer level, we have been keenly interested in these issues for many years.

I understand the Sub-committee is interested in hearing about Canada's approach to privacy as you consider the implications of the EU Data Protection Directive.

THE CANADIAN PRIVACY ENVIRONMENT:

Part of Canada's electronic commerce strategy recognizes that the future growth of the information highway will allow Canada to capitalize on the full potential of electronic commerce, with its ensuing economic and social benefits. We have recognized that in order to ensure that business and consumers fully embrace electronic commerce, building trust is critical and building trust means providing reasonable protection of personal information and privacy. At the same time, in order for Canada to become a leader in the global knowledge-based economy, the cost for business of managing personal information must also be reasonable and manageable.

This concern about protecting personal information has attracted the interest of governments around the world and a number of options to address the issue have been debated in various circles. One approach is to adopt a comprehensive regulatory regime with a very detailed, prescriptive, all-encompassing set of privacy provisions that applies to all organizations in all industries. At the other end of the spectrum is an approach that relies almost exclusively on market forces with spe-

cific legislation on a sectoral basis to deal with the most serious abuses. The Canadian approach lies somewhere in the middle.

THE CANADIAN APPROACH TO PRIVACY:

In October 1998, the Governments of the OECD Member countries attending the Ministerial Conference (A Borderless World: Realizing the Potential of Global Electronic Commerce) in Ottawa, Canada, adopted the *Ministerial Declaration on Protection of Privacy on Global Networks* which reaffirmed the importance of protecting privacy and recognized that the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the "OECD Privacy Guidelines") continue to provide an international foundation for the protection of privacy on any medium. The technology-neutral principles of the OECD Privacy Guidelines have formed the basis of self-regulatory and legislative initiatives internationally for almost two decades and continue to represent an international consensus for the collection, use and disclosure of personal information in any medium.

Let me then describe how the Canadian approach to privacy has built upon and implemented these Guidelines.

a) The CSA Model Code for the Protection of Personal Information

In the early 1990s, the level of concern of individuals over their privacy in general, and their lack of control over their personal information in particular, continued to rise coincident with the increased use of new technologies. In the face of this, the Government of Canada encouraged the business community to create a new Canadian standard for the protection of personal information. As a result, a Technical Privacy Committee of the Canadian Standards Association ("CSA") was struck that broadly represented all key stakeholders: business, government and consumers. Those organizations that participated represented key industry sectors with vast consumer bases that had a large stake in establishing an effective standard for the protection of personal information, e.g. the telecommunications, cable, banking, insurance, credit reporting and marketing sectors.

After a series of deliberations, the CSA *Model Code for the Protection of Personal Information,* CAN/CSA-Q830-96 (the "CSA Code"), was finalized and released as a National Standard of Canada in March 1996. The CSA Code is based on the OECD Privacy Guidelines and therefore represents a global standard. A summary of the CSA Code's 10 Principles is appended as an attachment to this testimony.

The Bell Companies participated actively in the development of the CSA Code. The Code's ten principles represent a cohesive and balanced set of fair information practices that reflect the needs and concerns of all parties. The Code clearly recognizes individual rights to control and limit personal information use, reflects the legitimate needs of companies to use information for business purposes, and establishes corresponding obligations for organizations to be accountable, obtain informed consent, safeguard personal data, and be open about policies and practices. As a "model" code, the CSA standard represents a set of minimum requirements and allows for the tailoring of the standard to meet the specific circumstances of an organization.

b) The Personal Information Protection and Electronic Documents Act

Following development of the CSA Code, repeated surveys continued to underscore that Canadians were still concerned about the effect of new communications technologies on their privacy. While electronic commerce was starting to take off, many consumers were still reluctant to make purchases on-line because they lacked confidence in the security and privacy of on-line transactions. They were still unsure about what they could do or whom they could approach when something went wrong.

Faced with that environment, the Government of Canada's Industry Department undertook broad public consultations to explore the possibility of a legislative approach. These discussions revealed broad support for self-regulation assisted by framework legislation that would encourage industry groups to develop sectoral codes based on the CSA Code.

After much discussion and consultation with a broad array of representatives from government, industry and consumer groups, the Canadian government introduced in October 1998 draft legislation that was ultimately enacted in the form of the *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5 (the "*PIPED Act*") in April 2000. Its stated objective has been to establish harmonized national rules across the country. The *PIPED Act* is also intended to meet the adequate data protection requirements of the EU Data Protection Directive.

This new piece of privacy legislation, which comes into force in basically two stages, is directed at the private sector and requires all organizations that collect,

use or disclose personal information in the course of commercial activities to adhere to the CSA Code.

Like the United States, Canada is a federal state. The federal government's approach to privacy also reflects a rather unique approach to the federal/provincial jurisdictional issue. As of January 1st of this year, the Act applies to all federal undertakings (e.g. telecommunications, broadcasting, airlines and banking industries), and those provincial undertakings that disclose personal information outside the province for consideration. In 2004, the provisions will apply more broadly to all organizations that collect, use, or disclose personal information in the course of commercial activities, including intra-provincial transactions. However, where and whenever a province adopts legislation that is "substantially similar" to the *PIPED Act,* the organizations covered will be exempted from the application of the federal law and the provincial law will instead govern.

The purpose of the *PIPED Act* is to (s. 3):

> "... establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

Due to legislative drafting conventions, it was recognized that it would indeed be difficult to incorporate the CSA Code principles and commentary directly into legislation, without significantly altering the carefully negotiated wording of the standard and compromising the flexible approach embodied in the standard. As a result the government adopted a novel approach to legislative drafting by having the legislation require compliance with the CSA Code, which in turn is reflected in a Schedule to the legislation.

For the most part, the *PIPED Act* reflects a flexible approach that does not impose or mandate particular treatment of personal information. Rather, organizations can develop codes and practices tailored to their particular business circumstances. The very process of developing a tailored code forces an industry group or company to consider more thoroughly the manner in which to deal with information issues specific to its business activities. Furthermore, the process of developing a tailored code serves to educate participating industry sector members about their obligations and the need to develop corresponding practices and procedures.

The legislation also requires commercial organizations to identify the purposes for which personal information will be collected, used and disclosed, and to obtain the consent of individuals from whom such data is collected. Consent can be either express or implied, depending on the circumstances and the sensitivity of the information—again reflecting a flexible approach. Commercial organizations, therefore, determine the scope of their identified purposes and consumers either accept them by continuing to do business with the organization or reject them by withdrawing consent or "opting out" of a particular proposed collection, use or disclosure.

The *PIPED Act* establishes a federal Privacy Commissioner as its prime overseer. Individuals may direct to the Commissioner complaints about any aspect of an organization's compliance with the provisions relating to the protection of personal information in the *PIPED Act.* The Commissioner has general powers to receive and investigate complaints, including the summoning of witnesses and production of documents and other records. The Commissioner also has express powers to conduct audits and to attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation. In fact, in framing the *PIPED Act,* the Canadian federal government clearly envisioned the Commissioner in an ombudsman role, with the stated goal of obtaining a resolution of privacy disputes in a non-confrontational manner. The Commissioner also has a mandate to develop and conduct information programs to foster public understanding of the privacy provisions of the *PIPED Act.*

Unresolved disputes relating to certain matters can be taken before the Federal Court of Canada for a hearing. In addition to its normal powers, the Federal Court may order an organization to correct its practices and award damages to the complainant.

By enshrining the CSA Code in legislation, the Canadian approach to protecting personal information recognizes that market forces alone will not provide the reasonable assurances that consumers require. At the same time, it avoids unnecessary and costly regulation that could stifle the growth potential of new technologies and provides necessary flexibility to tailor specific privacy practices to the unique circumstances of specific industry sectors. In our view, the Canadian approach reflected in the *PIPED Act* strikes an appropriate balance between a consumer's de-

sire for privacy and the legitimate needs of business to collect and use personal information.

Rather than imposing a common, detailed set of requirements and standards to be rigidly applied to all organizations in all industries, the Canadian framework legislation, recognizing that personal information needs vary tremendously across different industry sectors, accommodates maximum flexibility consistent with fair information practices.

Most importantly, given the consensus process adopted, the CSA Code has the confidence of both consumer groups and the business community and represents, therefore, a fair and equitable basis upon which to build a legislative framework.

THE BELL COMPANIES' CODE OF FAIR INFORMATION PRACTICES:

Privacy and security of customer information is considered to be a key attribute of the Bell brand, and an important aspect of the relationship between the Bell Companies and their subscribers.

The Bell Companies have long been committed—and continue to be committed—to maintaining the accuracy, confidentiality, security and privacy of customer and employee personal information. This is reflected in existing privacy and confidentiality provisions found in various Company policies and in applicable service rules approved by regulatory agencies over the years. It is also reflected in the high regard and trust with which customers and employees view the management of personal information by the Companies.

Recently, the Bell Companies released the *Bell Code of Fair Information Practices* (the "Bell Privacy Code"—copy attached). The Bell Privacy Code is a formal statement of principles and guidelines concerning the minimum requirements for the protection of personal information provided by the Companies to their customers and employees. The objective of the Bell Privacy Code is responsible and transparent practices in the management of personal information, in accordance with the CSA Code and the new legislation.

The Bell Privacy Code stipulates that the Bell Companies can collect personal information only for the following purposes:

a) to establish and maintain responsible commercial relations with customers and to provide ongoing service;
b) to understand customer needs;
c) to develop, enhance, market or provide products and services;
d) to manage and develop their business and operations, including personnel and employment matters; and
e) to meet legal and regulatory requirements.

As is the Companies' current practice, customers will continue to be able to review company records that contain personal information about them and update/correct any information contained in such records. Customers will also continue to be able to challenge any of the Companies' compliance with the Privacy Code through the existing office of the Bell Privacy Ombudsman. The office of the Ombudsman, which was established in 1992 in order to deal with unresolved privacy-related complaints, has received very few such complaints in the ensuing years—an indication of the Companies' commitment to privacy protection and customer satisfaction.

In order to implement the revised Bell Privacy Code, each of the Bell Companies has embarked on a plan that incorporates four elements: communications, training, systems and audit. The Companies are informing customers of the Companies' respective privacy policies and the implications thereof in a number of ways. The introductory pages of the white pages directory, bill inserts to customers, web pages and point of sale brochures all provide descriptions of the Companies' privacy policies. Business Office client representatives are also available to answer any questions that subscribers may have with respect to privacy. Copies of the Bell Privacy Code and other related documents are also available through these communication channels.

In addition, the Companies are in the process of ensuring, through training and employee communications, that all employees understand and will uphold the commitments made in the Privacy Code and related documents. Particular attention is focused on employees who have routine access to subscriber personal information as part of their job function. All employees must sign-off annually that they understand the Privacy Code, and acknowledge that non-compliance with our privacy commitments could be grounds for dismissal.

The Companies have also undertaken a review of their information systems to ensure that the provisions of the Privacy Code will be adhered to. Finally, regular internal audits will be employed to ensure ongoing compliance.

The Bell Privacy Code will be reviewed at least every 5 years to ensure continued relevance and currency with changing technologies, laws and the evolving needs of the Companies, their customers and employees. New communications plans would precede adoption of any modifications to the Privacy Code.

Finally, we intend to use technology to educate individuals about privacy issues, assist them to remain anonymous in appropriate circumstances and to exercise choice and control over the collection and use of their personal information.

CONCLUSION:

In my view, the development by industry, government and consumers of the CSA Code has had a positive impact in influencing the Canadian government's approach to legislation in this area. The result is a piece of legislation that is flexible and far less intrusive and prescriptive than other possible legislative approaches. The Canadian legislation enshrines high-level privacy principles while avoiding unnecessary and costly regulation and providing necessary flexibility to tailor specific privacy practices to the unique circumstances of specific industry sectors.

As leaders within our industry, we are committed to fair information practices within our individual companies, and to new voluntary initiatives that will further strengthen the level of privacy protection afforded to our customers and employees. Public education combined with market-developed technological solutions tailored to consumers' concerns and market demand will assist in providing the most efficient and effective means to protect personal information.

The Bell Companies have supported the Canadian government's steps in pursuing a new model for the protection of personal information in the private sector, a model tailor-made for Canada which builds on the voluntary efforts of consumer groups, industry and governments.

We believe the best model in Canada for private sector privacy legislation is a strong and consistent framework of harmonized federal-provincial laws. Most importantly, only consistent harmonized privacy laws across all jurisdictions will provide the level of privacy protection that individuals seek and require for the growth of global electronic commerce.

The Bell Companies remain committed to working with governments to promote effective privacy protection within a broader societal context.

We wish you well in your deliberations.

CSA CODE—PRINCIPLES IN SUMMARY

Principle 1—Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Principle 2—Identifying Purposes: The purposes for which personal information is collected shall be indentified by the organization at or before the time the information is collected.

Principle 3—Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4—Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5—Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Principle 6—Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7—Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8—Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9—Individual Access: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10—Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Mr. STEARNS. Thank you, Mr. Henry.

Let me start off. Mr. Winer, if we enacted—if we had the European Union privacy laws, what would be the cost to American taxpayers, American businesses? I mean, just give me a little brief scenario here. I have got lots of questions, so—I mean, it is going to be burdensome from your testimony, but, I mean, is there any kind of statistical or quantitative——

Mr. WINER. I have never been able to find one, sir. I have asked the Europeans any number of times if they have ever done such a study.

Mr. STEARNS. Right.

Mr. WINER. I believe the Department of Commerce may have requested that information from the EU and never gotten any response back.

Mr. STEARNS. Okay. Ms. Lawler, your company has signed the safe harbor, and there is less than 20. So you folks are out there early. And so I guess the real question, why—can you sort of let us in with a trade secret, why haven't the other technical companies signed on to this safe harbor? We all respect and admire your company, and it is one of the bellwether leaders in the industry. Why are you way ahead? Why haven't the other people done it?

Ms. LAWLER. Let me answer that by saying last month I was at a workshop on safe harbor that was conducted in the Bay area, which by the way was extremely well attended by many large global and national concerns.

And what I heard in comments—I think the first thing to keep in mind is that while the safe harbor principles have been under discussion for a couple of years, the real final result that was available for American businesses to actually look at and evaluate what they needed to do to certify to the safe harbor has really only been available since November 1st.

Now, for Hewlett Packard, we really had a running start because we had such a strong set of privacy policy and associated practices before the actual safe harbor agreement was even ratified, partly through our work with the safe harbor—I am sorry—with the BBB Online folks and that privacy seal program.

What I heard from some of my peers in that area is that there is still concern about some of the jurisdictional issues. They are waiting to see the standard contracts that were discussed in the first panel, to see if that was a viable alternative.

Mr. STEARNS. The model directives, you mean?

Ms. LAWLER. Excuse me? I am sorry.

Mr. STEARNS. You are saying contracts.

Ms. LAWLER. The standard contracts that one would sign with each——

Mr. STEARNS. For safe harbor.

Ms. LAWLER. [continuing] protection authority.

Mr. STEARNS. Okay.

Ms. LAWLER. As opposed to safe harbor, evaluating that as an alternative. Some companies are actually looking at developing very elaborate express permission scenarios, very expensive.

Frankly, a lot of companies just simply are not as far along in their internal practices and take safe harbor and the principles outlined very seriously. And so I think it is going to take them some

time to evaluate where they are at, what they are doing, and it is probably about a year process for them.

Mr. STEARNS. Mr. Winer, does the safe harbor provide a prudent option for American companies to comply with the EU directives, in your opinion?

Mr. WINER. If you are a company with a complex corporate structure, it is going to be very difficult because of the—each company, each structure, is viewed to be a third party, and you have to agree not to transfer to third parties, which could include intra-company transfers. Of course, it can't apply to financials or telecoms because they are not within the jurisdiction.

I think it is up to each company. The fact that so few have so far chosen to sign on is a vote with your feet proof that to date it has not been an attractive option for most companies. I think it would be terrifically valuable if we were able to get a cost assessment—as an answer to the question you asked me—done by proper economists, properly trained people, to try and figure out what real compliance costs are likely to be.

I noted in the testimony of my colleagues from HP, they are doing a very great job, but they confessed, I believe, at one point that there are some areas that they are finding some difficulty in completely meeting the terms of the directive as they develop their processes. So it is going to be a bit of work for everybody, and potentially an expensive one. We ought to know the costs.

Mr. STEARNS. Ambassador Aaron, you stated that the provisions of the safe harbor had to be more flexible than the directive and address real-world information practices on a reasonable basis. Yet only 26 companies and organizations have signed up for the safe harbor. Does this suggest that safe harbor is not a reasonable option for American companies?

Mr. AARON. I think it is a very reasonable option, and I might say that since we have had some of our panelists here say that it was either too tough and onerous, and others said it didn't mean anything and would not help, I think we have probably hit the sweet spot in trying to put this thing together.

I think the main reason that companies haven't signed on yet is that it is very complicated, and they want to look at it carefully. I think you could tell, even from the discussion this morning with the European Data Protection Authorities, even there is some confusion on their part as to exactly how all of this would work.

Well, I would be careful, too. And we are advising our clients that the safe harbor is a good way to go but that they have got to be very careful in how they do it, and that they have got to be sure that it is going to apply.

My principal concern at this point has been the fact that the European Union has started to chip away at the safe harbor. First, in the final days of negotiation, they made changes to how employee data would be covered, making it much more difficult than the safe harbor ought to operate from the standpoint of enforcement.

There are suggestions now that the—from the data protection authorities that if you send a cookie from the United States to a computer in Europe, that this somehow creates a facility in Europe,

and, therefore, operates under European law, and, therefore, somehow the safe harbor doesn't apply; it has got to be European law.

Well, I talked to the Commission personally on this issue, and they were rather horrified by this conclusion because it has implications for taxation and a whole lot of other things. And they are going to seek to get this clarified, but it is the kind of uncertainty that I think causes companies pause.

Mr. STEARNS. My time has expired.

Mr. Towns?

Mr. TOWNS. Thank you, Mr. Chairman.

Let me continue with the Ambassador. Is there an organized effort by some in the business community to keep U.S. firms from signing on to the safe harbor?

Mr. AARON. I, frankly, don't know. I haven't personally encountered—I know there were some people toward the very end of the negotiation that raised some objections, some of them of the sort that we have heard here today. But I don't know of any organized effort to boycott it in any way.

Mr. TOWNS. Well, in a recent article in Computer World, a representative of Dun & Bradstreet said that safe harbor allowed that company to obtain waivers for data transfers so that it could consolidate a UK-based data center with one in New Jersey. Do you believe that safe harbor helps keep data firms and jobs in the United States?

Mr. AARON. Well, there is no question about it. If—you know, there are two ways to run a business. One is you can totally decentralize, and if you are dealing with European employee data, customer data, that sort of thing, if you just keep it in Europe, but—particularly if there is obstacles to bringing it back to the United States.

I have one client who is—that basically provides a service that involves employee evaluation, and they provide this service to companies all over the world. And so they get evaluations from superiors and subordinates and colleagues and self-evaluations, and so forth. They do all of this processing in the United States.

Now, if they are not a member of the safe harbor, they are not going to be able to be in business. Now, they can go toward contracts, but I think, as Mr. Winer indicated, these contracts are enormously onerous. The basic principles are the same as the safe harbor, but then they tack on a whole series of other things about rights, private action, and all the rest, that this is not going to turn out to be an attractive alternative.

So I think at this point you have basically got the safe harbor, you have contracts, and that is what you have got. And I think the safe harbor is a much more congenial, flexible tool, even though it may go further in some respects than we would like.

Mr. TOWNS. Anybody disagree with that? Yes? You have a comment on that?

The reason I—let me just say, the reason I ask that, not that I am interested in having a debate of any sort, but the point is that I just think this issue is just so serious that we need to make certain that we get as much information as possible before we move forward, because I am convinced that something is going to be done in this Congress. So I really want to get information.

Yes?

Mr. REIDENBERG. I would hope you are right that this Congress will do something to protect privacy in the United States. I guess I disagree with at least one statement, that in the absence of signing up for safe harbor the companies will not be able to transfer data back to the United States.

Article 26 of the directive has a series of derogations from safe harbor—or, excuse me, has a series of derogations from export prohibitions that are more extensive than simply having a contract between an American data importer and the European data exporter.

The other thing that I think the committee ought to be aware of is that the export prohibition provision did not begin with the European directive. It began with member state law that preexisted the directive for many years.

And many of the certainly larger American companies have been dealing with this as a fact of life for more than 20 years in some member states and have not had problems, because they have worked with the national data protection authorities in each of those member states, assuring them of treating the European data with fair standards in the United States.

So if it is a company that is treating data fairly in the United States, I find it very perplexing that they have such difficulty either signing onto a contract for data protection or subscribing to something like the safe harbor, the substantive standards of the safe harbor.

If they are indeed practicing privacy, these obligations should not be that—should not be burdensome for them. Again, keeping in mind if they are operating in Europe, they are under legal obligation in European countries to do that anyway.

Mr. TOWNS. Thank you.

Yes, Mr. Winer?

Mr. WINER. Yes, sir. I would say that the devil is in the details in this area. And one of the reasons why so few companies have signed up is because you have to do a very detailed analysis of how the safe harbor applies to your actual operations and information systems. And if you have got a complex corporate structure or complex sets of information, you may not be able to live up to the safe harbor very easily. It may be expensive and difficult.

So its value is very fact-dependent, and there are lots of gaps.

Mr. AARON. May I just add one point? This is true of any privacy policy. And one of the great and surprising things is that if you would talk to most companies about the privacy policy, you can often find out that they just borrowed it from some other company. They just went on the web, took the privacy policy, stuck it on there. It has nothing to do with their business.

You talk to general counsels of major corporations about their privacy policy, and you ask them, "Do you collect personal data? And who do you share it with?" And they say, "We will get back to you," because they don't know. They have to go all the way down to the data base managers and find out what is really happening in those companies.

This is true of any privacy policy. It goes to the heart of most companies and business operations, and it is a crucial thing, and it is going to cost money for everybody.

Mr. TOWNS. All right. Mr. Chairman, my time has expired.

But let me commend Ms. Lawler for her company in terms of their moving forward. I just wanted to let you know that we salute you for that.

Ms. LAWLER. Thank you, sir.

Mr. TOWNS. Right. I yield back.

Mr. STEARNS. Mr. Buyer is recognized for 5 minutes.

Mr. BUYER. Thank you, Mr. Chairman.

Ms. Lawler, I have got your web page. Okay?

Ms. LAWLER. Okay.

Mr. BUYER. One thing I do like about it, what appears to be open and conspicuous, and I don't know if it is redundant, but over here it says privacy statement. So you can click on it, right? And you get over into it, it says, "Who do we share it with?" i.e. obviously, the personal data.

So you want to get in there, and it is—I heard your testimony. It sounds good. So let us examine what you said. HP will not sell, rent, or lease your personally identifiable information to others. And that is what your testimony was.

Ms. LAWLER. Correct.

Mr. BUYER. Okay. Now let us go into the but. You then give permission to your partners——

Ms. LAWLER. What I said in my testimony is that we will not share with partners without customer permission. I can share some examples if you would like.

Mr. BUYER. [continuing] that you provide online with other HP entities and/or business partners who are acting on behalf, and the uses are described, how we use it.

Ms. LAWLER. Business partners acting on HP's behalf. That was the scenario I described where their suppliers and service providers—they are required and covered under contract and on disclosure to abide by our privacy policy.

Mr. BUYER. So all of your other subsidiaries or partners whom you do business with, you go all the way back to your customer. If I click on—my son clicks on and does something with HP, you are not going to give any of that data unless you go back and ask whether or not you can give it?

Ms. LAWLER. What that is saying is that if they are covered under contract, they are covered by the privacy policy. An example would be an advertising agency creating material for us or a shipper like, say, Federal Express shipping our product.

Mr. BUYER. Let me ask this. Do you believe that there should be a level of comfort with someone who would use your site, that the information or their practice is not going to then be shared with your other business partners or arrangements or contractual partnerships that dominoes one after another?

Can I turn to my constituents and say, "Hey, what HP says is when you deal with them, none of that information is going to be shared with anyone else unless they come back to you"?

Ms. LAWLER. If you are referring to the situation we talked about with suppliers——

Mr. BUYER. No, no, no, no. Don't go to what your situation is. Go to mine. See, I don't believe——

Ms. LAWLER. Can you give me a specific——

Mr. BUYER. I don't believe you can stand by what you just said. That is what I am questioning. First, you give that one statement that is pretty emphatic, and then you go into the "unless." I always pay attention to the unless, however, but, comma.

Ms. LAWLER. That is not a but or unless, but I understand what your question is.

Mr. BUYER. All right. I don't want to quibble with you.

Ms. LAWLER. Okay.

Mr. BUYER. I just want to get the definition.

Mr. STEARNS. Will the gentleman yield for just a moment?

Mr. BUYER. Yes.

Mr. STEARNS. Another question you might ask is, how are they enforcing against their partners?

Mr. BUYER. Well, that is the real problem. If you have information which you say, "Well, we are going to give it to one of our business partners," then you begin to lose control when that business partner has a second arrangement with another business partner, and all of a sudden it is three, four down the line and you have——

Ms. LAWLER. Okay. I need to go back to what I had been saying, which is that if it is a partner doing business on behalf of HP—in other words, we could have our own shipping organization that delivered packages to your door, we could have an in-house ad agency, we could have all in-house call centers for an example. An alternative is to outsource that effort.

Outsourced efforts are covered under contract and legal non-disclosure agreements that the vendor—this is a vendor-supplier relationship—that they sign. Therefore, they are protected. So they have the data, but they are not using it for their own business purposes. They are using it on behalf of HP contractually; therefore, legally protected.

That is different from a business partnership, say, for example, with a software supplier. Say, for example, you bought a Hewlett Packard Pavillion PC, and you decided to register that product with Hewlett Packard, which, by the way, is your choice. You can also choose to register your software applications at the same time in one single approach, which many customers see as a benefit. Others prefer to register individually.

So if we think of a major software provider, we provide you the option to transmit your personal data to that software provider to complete the registration process in one single effort. But we ask that permission question before that happens. And if you don't want to do that, it doesn't happen. You are in control.

Mr. BUYER. Thank you.

Mr. STEARNS. The gentleman from Tennessee, Mr. Gordon?

Mr. GORDON. Thank you. We only have 5 minutes just like you do, so I am going to try to be quick with three questions and hope you will be quick with three answers, or at least the first two.

Ambassador Aaron, if you could help maybe clear up a question I had raised earlier concerning the safe harbor, and that is that if a company is within safe harbor, then FTC makes those determinations. My concern is, then, does the—is there a veto or an override in some regard by any of the EU countries to say that the FTC is not doing their job properly or they don't agree?

Mr. AARON. No, there isn't. Now, having said that—and that is part of the deal. Having said that, if Mr. Rodotà, for example, should decide he didn't agree with that and he thought that some U.S.—some firm in Italy was sending information to a company in the United States that wasn't behaving properly, and he moved to enjoin that transmission of information, then it would be the responsibility of the European Commission to go after Mr. Rodotà and to get together his various committees and make a determination as to whether Mr. Rodotà was in his rights or was not.

And they have made clear to us, in the course both of the negotiations, that they would move to insist that the national data——

Mr. GORDON. So they can overrule the FTC.

Mr. AARON. They can overrule the——

Mr. GORDON. Well, that is all I wanted to——

Mr. AARON. They can overrule the national—the Commission can overrule the national Data Protection Authority.

Now, anybody can sue anybody. If somebody goes into court and says, "I am not being protected in a European court," then the European Commission will weigh in on the side of the U.S. defendant if they are within the safe harbor.

Mr. GORDON. But they still can overrule the FTC, the individual countries, can't they?

Mr. AARON. No, they cannot. The European Commission comes in and declares that action illegal or unacceptable.

Mr. GORDON. But isn't that the same thing?

Mr. AARON. No. The action of the member state is illegal or unacceptable. In other words, any——

Mr. GORDON. But can they rule that it is acceptable, their action is acceptable?

Mr. AARON. Well, I suppose that is conceivable, but then that is a violation of our agreement and that raises everything to a political level and we begin to——

Mr. GORDON. So why would—okay. Well, maybe I just need to understand that more.

Mr. Winer, you gave a lot of reasons why the EU should not go forward with the regulations that they have. Is there any reason that they can't make a bad decision? I mean, you said it is a bad decision. But do they have the right to make that bad decision?

Mr. WINER. They certainly have the right to make a bad decision. The question is, what is the U.S. response when another country makes a bad decision?

Mr. GORDON. That is the main thing I wanted to know.

Mr. WINER. Yes, sir.

Mr. GORDON. So they have the right to make that bad decision.

And, finally, if I can—Mr.—I guess this is—Mr. Reidenberg, if I was a—from a business perspective, what makes me most concerned about dealing with the EU would be the uncertainty as well as maybe the arbitrariness of how some of the rulings, you know, could be arbitrated.

I think you have what I would think is the best suggestion, and that is some type of international treaty which would go beyond EU into problems around elsewhere. What would be the vehicle for that international treaty?

Mr. REIDENBERG. The WTO, in particular, Telecoms Annex.

Mr. GORDON. Yes, okay.

Mr. REIDENBERG. There is a specific exception for restrictions on trade and services and information under the Telecoms Annex for privacy. And the WTO agreements require biennial assessments at a ministerial level for——

Mr. GORDON. Is there any kind of effort going on to develop some international standards in that regard?

Mr. REIDENBERG. There has been some suggestion that the WTO take it up. To my knowledge, that has not yet happened. I think it is inevitable that the WTO will have to focus on privacy issues. I would prefer to see the United States taking the lead than being the second seat at the table.

If I may for a moment refer specifically—this goes back to your first question that you raised with Ambassador Aaron. Article 3 of the Commission decision of July 26th, which is the decision approving the safe harbor, specifically allows the member state data protection authorities to reject transfers to a company on the safe harbor list.

So the specific answer is Article 3—it is specifically Article 3, clause 1(b), specifically says that the member states under certain circumstances can refer to recognize a company on—listed on the Commerce Department's listing of certified safe harbor companies.

Mr. GORDON. Well, that was my understanding.

Ambassador Aaron, I guess you can say it, but maybe I don't understand it, I mean, why do you see this differently than the rest of us?

Mr. AARON. Because the Commission has further powers. The Commission has the power to look at any decision made by a national Data Protection Authority and decide whether it is within the scope of the safe harbor or whether it is doing something aberrant. It has nothing to do with the safe harbor, trumping the FTC, doing something——

Mr. GORDON. Right.

Mr. AARON. [continuing] of that sort.

Mr. GORDON. So however you get there, but that is the same result. I mean, that they can overrule the FTC, can't they? But why don't you maybe——

Mr. AARON. No.

Mr. GORDON. Again, I am just wondering, why do you see this differently than everyone else here?

Mr. AARON. I guess maybe because I negotiated it and I know what those words mean.

Mr. GORDON. Or is that just editorial pride?

Mr. AARON. No, I don't think so. I don't think so. I don't think I actually wrote the words.

Mr. GORDON. Okay.

Mr. AARON. What happens is that if the national—there are some exceptions, as you pointed out. But, basically, if the national data protection authorities do not recognize the safe harbor, the Commission has the right to come in and make them recognize it. That is the deal. So if they do something——

Mr. GORDON. They have the right to, but does that mean that they have the obligation to?

Mr. STEARNS. The gentleman's time has expired.

Mr. AARON. Well, that——

Mr. GORDON. I mean, if they don't have the obligation to, then it doesn't really matter, does it?

Mr. AARON. Well, they actually have the obligation to under their own rules.

Mr. GORDON. Thank you.

Mr. STEARNS. The gentleman's time has expired.

The gentleman from Georgia, Mr. Deal, is recognized for 5 minutes.

Mr. DEAL. Thank you, Mr. Chairman.

Mr. Henry, as I understand, what has happened in Canada is you started out with industry code that was industry derived, and that has now been backed up with legislation, but the legislation is very flexible and embodies the possibility for many variations of types of agreements. Is my understanding correct?

Mr. HENRY. Flexible in the sense that it allows—it sets out a number of obligations. But the manner in which you meet those obligations or fulfill them leaves some flexibility. So, for example, different industries, it actually envisages that different industries would develop different practices to reflect the particular business circumstances, still complying with the principles and having an obligation to comply with the principles.

And consent as well is a flexible concept. The form of consent depends very much on both the sensitivity of the information and the circumstances, and so on.

Mr. DEAL. But these are national standards with——

Mr. HENRY. Right.

Mr. DEAL. [continuing] the right of territorial——

Mr. HENRY. Right.

Mr. DEAL. [continuing] variations.

Mr. HENRY. Right.

Mr. DEAL. I guess the next question, then, is, has the EU acknowledged your legislation and your code as an acceptable compliance with their directive?

Mr. HENRY. It is in the process of doing so. There is a couple of working group studies underway. I think Mr. Smith earlier acknowledged that it looks like they will accept it, and certainly——

Mr. DEAL. Will it be a blanket approval, or will it—since there is flexibility, would it be a case-by-case determination?

Mr. HENRY. Well, our hope and understanding, and the Canadian government's hope and understanding, is that it will be accepted. The EU is looking at it, and once they understand it we are confident that they will accept it. Yes, absolutely. And it was drafted not only with that in mind but certainly with that in mind, that it was to comply with the EU directive.

Mr. DEAL. All right.

Mr. HENRY. And if I could just add one other thing. When I say "flexibility," it is flexibility on those points I talked about. On the enforcement side, I think it is much stricter. There is a privacy commissioner with a lot of power. There is possibilities to go to court. There is audits. There is public reports that the privacy commissioner can make. So it is quite strict in that sense.

Mr. DEAL. Professor Reidenberg, I believe your suggestion of trying to arrive at some standard initiated that would be acceptable

to our country, and then going through WTO to see if we could arrive at a mutually agreeable standard, is probably a very good approach.

But your comments also indicate that if American companies are really doing basically what they should be doing, they really shouldn't have that much trouble under the current arrangement, even though it is somewhat disjointed. Is that a fair summary of what I heard you say?

Mr. REIDENBERG. Yes and no. I think it is a fair summary, but it probably doesn't completely present an accurate picture. If American companies were doing what they were supposed to be doing, and by that I am going to treat that as an American standard, if companies were treating information fairly with the kinds of principles that we have long recognized in the United States going back to the OECD guidelines from the early 1980's, if they were doing that, then substantively they should be in compliance with the kinds of obligations that the European directive imposes.

It would not, however, alleviate the practical problem of having to prove their adequacy on a case-by-case basis, because there would be no obvious legal right to point to, no obvious enforcement ability to point to. They would have to go and show case by case, yes, we are doing these things. So——

Mr. DEAL. Mr. Winer, or Ambassador Aaron, do either of you disagree that going to a standard—WTO approved standard would be not a desirable goal to try to shoot for? Or is there a better way?

Mr. AARON. I think there is a better way, and I think the better way was reflected in the testimony we heard earlier, which is a thing called the global business dialog for e-commerce. They are in the process of developing a number of private sector, international rules and standards, much along the lines that the Canadian private sector did, kind of a code of conduct.

I think that is likely to be much more flexible, much more effective, much more widely accepted, and to try to go into an organization of 140 or 70, or I don't remember how many members there are now, including China and a couple of other countries, and try to negotiate privacy, this is not going to be an easy thing to do.

Mr. DEAL. Thank you, Mr. Chairman.

Mr. STEARNS. Thank you. I think—there are just a few of us left—we will take another quick round. Make sure you don't miss your planes.

Mr. Henry, it seems like Canada has developed something with the participation of industry. So industry came in and participated in developing the code and practices, as I understand it, that is tailored to the different industry that applies.

Did you find that industry's participation made it less burdensome? I mean, that relationship, did that make it palatable for them to take an all-encompassing law? I mean, you might give us just a little——

Mr. HENRY. Absolutely. What they did was develop a code that was at a higher level, and that code is a single code. That is a CSA Code. But that code itself allows and envisages that industry-specific sectoral codes could be developed to be in compliance with that code. And so——

Mr. STEARNS. Ambassador Aaron, you mentioned the global business dialog of e-commerce. So if you were in a position where you could wave a magic wand and put in place, for the United States or for world commerce, one consistent privacy practice, how would you do it, and what would it be?

Mr. AARON. Well, I think that the basic principles that were contained in the OECD privacy principles are a good place to start. But it is very important to recognize that different sectors of the economy have different privacy requirements and need different kinds of flexibility.

So I would build from there, but I would try to realize that there are sectoral differences. For example, the Europeans don't accept our Gramm-Leach-Bliley and Fair Credit Reporting Act. I think this is a big mistake on their part. We provide tremendous——

Mr. STEARNS. They don't accept our what?

Mr. AARON. They don't accept that the Gramm-Leach-Bliley privacy protections and the Fair Credit Reporting Act protections——

Mr. STEARNS. Oh, okay.

Mr. AARON. [continuing] are adequate.

Mr. STEARNS. Okay.

Mr. AARON. They think that is not adequate privacy protection. I think that is entirely unacceptable for us. And, of course, we are going to come to the crunch on this issue pretty soon. But those two acts working together provide tremendous privacy protections, and they are enforced by the Fed and by the Office of Thrift Supervision and all the rest of it.

But I really think you can't just spell out—well, I would be happy to do it at some point, maybe write a book about it, but I think you really have to think about—you know, you have to give notice; how much? You have to give choice; opt-in/opt-out. You have to talk about third parties and your obligations.

Mr. STEARNS. Do you think in opt-in or opt-out there is a favorite in your mind?

Mr. AARON. I think that opt-out ought to be quite acceptable for many, many purposes.

Mr. STEARNS. So——

Mr. AARON. And, in particular, let me just say one thing. You know, the debate that took place in Gramm-Leach-Bliley, during that period, was whether there should be opt-in for sharing with affiliates. That was the big fight over that issue.

Well, the Europeans say, "No, you have to have"—what we were trying to do with that was to try to make us equal to the Europeans. The European banking institutions and financial institutions aren't structured the way we are. They have insurance. They have brokerage. They have banks. They are not affiliates. They are actual divisions of a company. So, therefore, they share this between each other all the time, with no difficulty.

We are structured—many of our companies are structured differently. So all of a sudden you get this issue of affiliate sharing, and whether there should be opt-in or there should be opt-out. Well, I think we have got to be careful there because the fact of the matter is if we accepted either one of those procedures—and we did accept opt-out to some extent—we find ourselves at a competitive disadvantage.

Mr. STEARNS. Mr. Winer and Professor Reidenberg, both of you briefly tell me what you would do if you could wave a magic wand to get this privacy so that it would be a global business policy.

Mr. WINER. For starters, the EU needs to recognize the US system for protecting privacy as adequate. Our system protects privacy in practice better than the EU system. You go in, you get privacy policies——

Mr. STEARNS. So they have got to recognize the Gramm-Leach bill.

Mr. WINER. Absolutely. And Fair Credit Reporting. You look at the privacy policies companies put online. If you don't do that, you are going to have customer problems, you are going to have FTC problems, you going to have Attorney General problems.

We have a system in this country of regulation and enforcement that is very aggressive. You go over to the EU they have got soft guidelines, and they have got much less enforcement. They don't have regulations for the most part.

And the testament is, you get the consumer groups looking at it, and they are saying, "Yes, America actually does it better, even though the EU standards are tougher." So the first thing would be they have to recognize our system and give due respect to our system. Yes, sir.

Mr. STEARNS. Okay. Professor?

Mr. REIDENBERG. I think it is nonsense that Gramm-Leach-Bliley meets the standards contained in the European directive. I think we are bandying about the term "adequate" in different ways. Adequate, under the directive, means does it satisfy the obligations contained in the directive.

We may talk about it as being adequate for the American context as an enacted by Congress. I personally have views much more akin to Mr. Markey's from this morning. But in terms of the Gramm-Leach-Bliley compared to the standards in the directive, Gramm-Leach-Bliley is essentially a notice and consent statute. The directive contains substantially more than that in terms of fair information practices.

It contains data subject access rights. It contains security rights. It contains a whole host of things that Gramm-Leach-Bliley is just simply silent on.

Similarly, the Fair Credit Reporting Act is a very important piece of privacy legislation in the United States. But if you look at it carefully in the context of the directive, and if you look at it carefully in its own context, it has the most tortured set of definitions for what is covered under the Fair Credit Reporting Act of any recent legislation we have had.

What I would do in the United States, I would enact the OECD guidelines and statutory obligations, and I think we need to look at some creative ideas like creating a mechanism such that—a safe harbor mechanism so that companies have a degree of certainty in particular contexts what their obligations are under a statutory enactment like the OECD guidelines.

Mr. STEARNS. My time has expired.

Mr. Towns?

Mr. TOWNS. Thank you very much, Mr. Chairman.

Mr. Winer, I see from your statement that in the previous administration you served in the State Department and were engaged in negotiations with the EU. When you were at the State Department, were you a member of the United States delegation that negotiated the EU-U.S. safe harbor agreement?

Mr. WINER. No, sir.

Mr. TOWNS. So you are not appearing at this hearing as an expert witness based on any direct involvement in those negotiations. Is that correct?

Mr. WINER. In those negotiations, no, sir. I did lots of other negotiations with the EU, however, sir.

Mr. TOWNS. Your written statement says that you are affiliated with the law firm of Alston and Byrd, and that you spend much of your time, "Counseling U.S. companies about privacy issues," including the EU privacy directive that is the subject of this hearing today.

Are you representing clients this afternoon in your appearance before the subcommittee? And, if so, who are they?

Mr. WINER. No, sir, I am not. These represent my views. No one from outside my law firm reviewed any aspect of my testimony prior to my writing it. It reflects my views. In fact, it reflects opinions that I held when I was in the Clinton Administration.

Mr. TOWNS. Okay. Well, do your clients want to see the safe harbor agreement terminated?

Mr. WINER. I have not asked that question of any client, if they want the safe harbor agreement terminated. I think what people want is a safe harbor that is going to work for them.

I think what they want is respect for—when you are in compliance with U.S. law, that you are not going to be punished for when you act in compliance with U.S. law by somebody else, and that your compliance with U.S. law will buy you some protection against being punished elsewhere. I think that is what some people would like to see, sir.

Mr. TOWNS. All right. Thank you.

Ms. Lawler, you know, I am still back on the question that Congressman Buyer raised, if there was a violation. It is my understanding that if HP would actually be liable to its consumer if that occurred, and it would be my understanding that then HP would go after the vendor, is that correct?

Ms. LAWLER. Correct.

Mr. TOWNS. Yes. So I couldn't quite understand where he was going with that. That was really, you know—I couldn't quite, you know—well, anyway, that is another issue. I am sorry he is not here, because I don't want to pursue it any further because I am sure he would have, you know, maybe a response. It is unfair I think to pursue it, you know, because of the fact that he is not present. But I just had to say that because I have thought about it.

The other thing is that, basically, I wanted to raise with you, Ms. Lawler, it is my understanding that the EU has tried for years but so far has failed to agree on what a model privacy contract should look like. Nevertheless, contracts are being entered into every day.

Do U.S. companies have sufficient commercial presence in the EU that they can hold their own in these contract negotiations? Or

does the absence of a model contract mean that our companies are at the mercy of EU privacy directives?

Ms. LAWLER. I think the companies that are looking at this issue have significant presence in Europe, and not just in Europe, quite frankly, and have fairly sophisticated groups, both in legal and contracts, that certainly could hold their own if they chose to pursue that particular route.

I know for Hewlett Packard we made a very distinct business strategy decision not to get into the contracts business if you will. Our business, as many technology companies—business changes so rapidly that you are essentially in an ongoing contract discussion that never ends. And we didn't feel that was a good business model for us.

Mr. TOWNS. All right. Thank you.

Professor Reidenberg, let me say we have something in common. You know, I was on staff at Fordham as well, I want to let you know, so we have that in common.

Now I will ask you the question. The international treaty that you talked about to solve the privacy issue, what is the timetable, the timeframe, with that? You know, because when you think about these kinds of things you think about, you know, something going on and on and it might not even happen during my lifetime.

Mr. REIDENBERG. I can't predict how long it would take to negotiate such a treaty. It certainly would not happen overnight. But then, if we look at the basic privacy principles that the United States domestically has committed to over the years, and those in the directive, they have been around for 30 years. They have been pretty enduring. So my guess is it would take a couple of years to negotiate it.

At the WTO, they will—as I said, I think it inevitable that they will have to focus on privacy in the context of the trade and services assessments that take place every 2 years. Now, whether it will be this year or next year, I couldn't tell you, but I think it will be imminent that this will have to be on the agenda.

Mr. TOWNS. Thank you very much, Mr. Chairman. My time has expired.

Mr. STEARNS. I thank my colleague.

Mr. Deal, you are recognized for 5 minutes.

Mr. DEAL. Thank you, Mr. Chairman.

Well, I omitted saying at the outset thanks to all of you for being here. I think we have heard some very good testimony and certainly this panel and the preceding panel have given us information that is important in our deliberations.

But I suppose always there is, from our perspective, the question of, what is the starting point and what is the goal? And I have heard very divergent goals set forth here, and I guess I am probably at this point in time coming down on the side of saying that our approach maybe should be something similar to what the Canadians have some, and similar to what—the position Mr. Winer has advocated.

And that is, once we have legislatively determined what standards we feel are acceptable and agreeable for our constituency as citizens of our country, then we then move to the next stage of, do our trading partners agree with that? And if they don't, then what

modifications, if any, should we come to? And, of course, we have not fully come to those conclusions.

And, obviously, Professor Reidenberg, I have a connection, too. My son-in-law is a graduate of Fordham, so we will make that connection.

But, obviously, yours is a much more long-term goal of having something in a more international context whereby you would have an agreement that was enforceable. But for the immediacy of the problem, I think we would all recognize that that is fraught with great difficulties.

Obviously, some who are members of WTO think that government should know everything, and some of us think they should know nothing. And I think it would be very difficult in a short timeframe to come to a standard that would perhaps be acceptable without major deviations from it or exceptions carved out of it.

I think from my perspective, our focus should be, in the short term, let us decide what standards our people want, and then, if at all possible, try to mesh those with our trading partners as they now exist. If those can be done, it seems to me then we have a very workable base from which to move to a broader WTO-type concept. Am I looking at it in an unrealistic fashion?

Mr. AARON. I don't think so, Mr. Deal. I think that one of the difficulties that I had in negotiating the safe harbor is that we really didn't have anything to sort of say, "This is where we are."

Mr. DEAL. Right.

Mr. AARON. And so I had to kind of negotiate off of their sheet of music. It would have been much better for me, as well as I think for the country, if we had had something of our own.

The one thing, I would make one comment about the Canadian rules. They are really designed—they are very much in the mold of the European ones, and they have very strong enforcement provisions. And that is the one thing that I think is going to be very difficult for the United States.

We looked at this back in the 1970's, at an idea of a comprehensive privacy program, what the privacies are, and all that kind of stuff. And we came to the conclusion that this might well threaten people's privacy. I mean, somebody independent——

Mr. DEAL. We don't want to tell anybody, so he can decide.

Mr. AARON. Yes. I mean, this is—so that very key thing—and that is the key thing that makes it acceptable to the Europeans. So we still have something resembling a square that needs to be circled.

Mr. DEAL. Mr. Winer?

Mr. WINER. Yes, sir. I think if you think of the U.S. approach with consumer issues, it is very often an approach of fairness in which you want to say, "Has the person been informed about what is going to happen? Has the person consented to what is going to happen?" If you have got a situation where somebody has been informed and consented, that tends to be acceptable in American commercial and consumer context in many, many situations.

Now, of course, there are situations at the very extremes where you want to go beyond that. But informed consent is the heart of our system, and seems to me might be a basis for proceeding here, sir.

Mr. DEAL. Professor?

Mr. REIDENBERG. Let me come back I think first to your original query. I think you are absolutely correct. We first have to get our house in order and deal with privacy in the United States.

Part of—and I agree completely with Ambassador Aaron, part of the difficulty in dealing with the rest of the world right now is that the rest of the world is looking to Europe for leadership on privacy and is no longer looking at the United Sates. We used to be the leaders. That is no longer the case.

So I do think we do, first, indeed have to focus on what are the kinds of rights for the American democracy that we need to protect in the context of privacy. And in that context, we have to do more than just give window-dressing privacy. We need enforceable rights that have legal remedies for individual citizens who are victimized. That is something that is also very typical in the American context.

And I think that in this area in particular there are some instances where informed consent is not likely to be satisfactory for us. We find privacy is a political right. Privacy has very important political implications, and we don't in the United States allow selling of votes. There are instances where we should not be in the position of forcing citizens to sell their privacy so that they can get an extra couple of dollars off. That essentially says rich people have privacy and poor people don't, and I don't think, as a society, we should accept that in the United States.

Mr. DEAL. Thank you, Mr. Chairman.

Mr. STEARNS. I thank my colleague, and I thank panel two, especially for your patience in waiting when we went through over an hour of voting. I appreciate your attendance, and I thank my colleagues for staying with us. This is very nuanced debate that will continue.

With that, the committee is adjourned.

[Whereupon, at 3:13 p.m., the subcommittee was adjourned.]